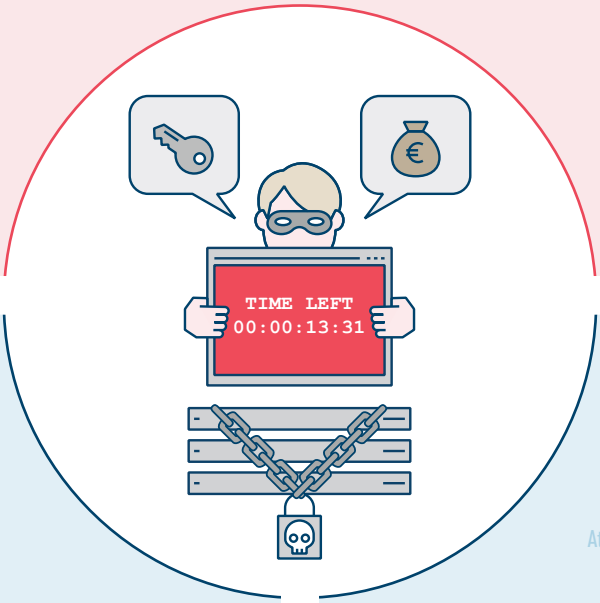
RANÇONGICIEL

Vos données sont prises en otage

QUE SE PASSE-T-IL ?

1. Vos données sont progressivement chiffrées, ce qui les rend inaccessibles



2. L'infection peut s'étendre à tous les appareils connectés au réseau ou aux supports USB branchés

3. On exige de vous le paiement d'une rançon pour récupérer ces données

Impact de l'attaque

- Intégrité
- Authenticité
- Disponibilité
- Confidentialité

Motivations principales

- Atteinte à l'image
- Appât du gain
- Nuisance
- Revendication
- Espionnage

COMMENT RÉAGIR ?

Vous êtes victime d'un rançongiciel – Ne payez pas !

1- Ne pas éteindre la machine concernée
La mettre en veille prolongée si possible

2- Déconnectez immédiatement les appareils du réseau

3- Ne connectez plus aucun appareil sur le réseau

4- Contactez immédiatement votre service informatique ou un expert (ou trouvez le vôtre sur cybermalveillance.gouv.fr)

5- Portez plainte auprès des services compétents

COMMENT SE PROTÉGER ?

Ne tombez pas dans le piège

Effectuez des sauvegardes régulières de vos données.

Mettez à jour régulièrement vos principaux logiciels
- Les rançongiciels utilisent les vulnérabilités des programmes pour se propager

Privilégiez un compte utilisateur pour vos usages courants

Courriers électroniques piégés
- Ne faites pas confiance à l'expéditeur de courriers électroniques dont l'origine ou la forme vous semblent douteuses
- Méfiez-vous des pièces jointes et des liens suspects

#CyberVigilant ! En savoir plus sur les attaques par rançongiciel :
https://www.cert.ssi.gouv.fr/information/CERTFR-2017-INF-001
https://www.cybermalveillance.gouv.fr/nos-articles/les-rancongiciels-ou-ransomware/

Les bonnes pratiques de l'informatique : www.ssi.gouv.fr/precautions-elementaires/
En savoir plus sur l'ANSSI : www.ssi.gouv.fr
En savoir plus sur Cybermalveillance.gouv.fr : www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

V.4-20180119-1930