



# LES RANÇONGIERS

CYBERCRIMINEL



## EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

### BUT

Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

### TECHNIQUE

Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.



VICTIME



## COMMENT RÉAGIR ?

- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corrigez l'origine de l'infection
- Essayez de désinfecter le système et de déchiffrer les fichiers
- Réinstallez le système et restaurez les données
- Faites-vous assister par des professionnels

*Pour en savoir plus ou vous faire assister, rendez-vous sur [cybermalveillance.gouv.fr](http://cybermalveillance.gouv.fr)*

## LIEN UTILE

[www.nomoreransom.org/fr/index.4html](http://www.nomoreransom.org/fr/index.4html)

## DISPOSITIF NATIONAL D'ASSISTANCE AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE

Assistance aux victimes  
Information et sensibilisation  
Observation du risque numérique



avec

MINISTÈRE DE LA JUSTICE

MINISTÈRE DE L'ÉCONOMIE  
ET DES FINANCES

MINISTÈRE DE L'INTÉRIEUR

SECRÉTARIAT D'ÉTAT CHARGÉ  
DU NUMÉRIQUE

**RETROUVEZ TOUTES NOS PUBLICATIONS SUR :**

[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

