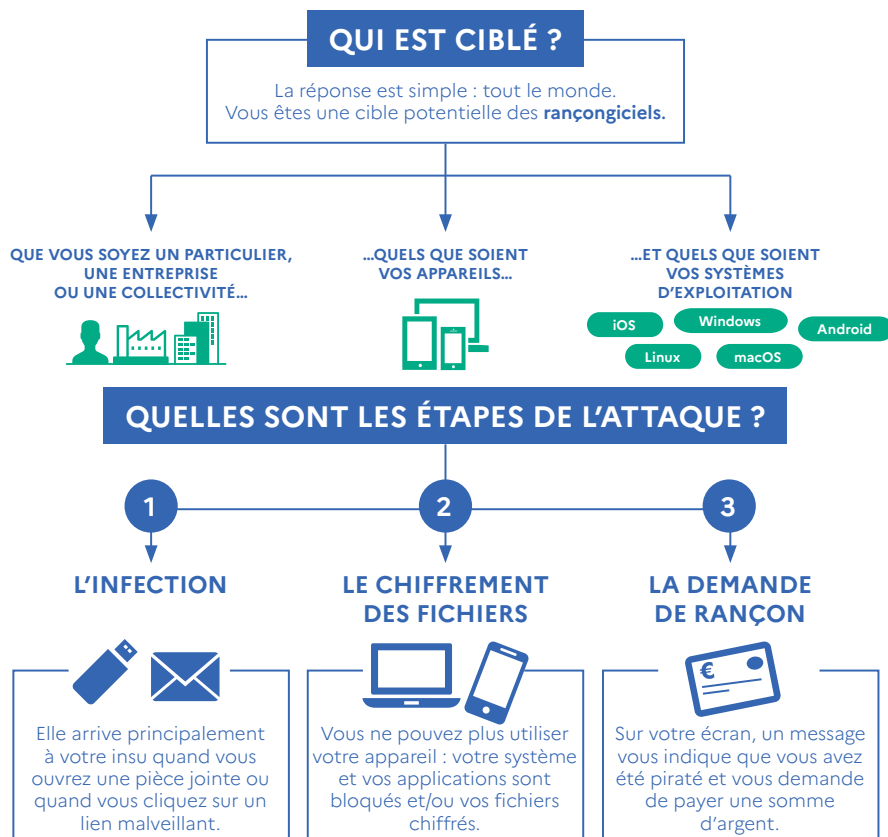


LES RANÇONGIERS



GandCrab et LockerGoga récemment ; WannaCry, NotPetya ou encore SamSam il y a quelques années... Les rançongiciels (ou *ransomwares*) sont au cœur de l'actualité. Mais les connaissez-vous vraiment ? Un rançongiciel est un logiciel malveillant qui bloque votre ordinateur et rend tous vos contenus informatiques inaccessibles. Il s'agit d'un virus informatique qui permet aux cyber-attaquants d'accéder à ces fichiers et de réclamer une rançon aux victimes pour qu'elles puissent récupérer l'accès à leurs informations personnelles / leurs fichiers.



POURQUOI NE FAUT-IL PAS PAYER ?

Même si vous réglez le montant de la rançon, rien ne vous assure que vos fichiers seront déchiffrés ou que votre ordinateur sera de nouveau accessible. De plus, vous alimentez un système et démarrez un cercle vicieux : après avoir payé, vous risquez d'être identifié comme « bon payeur » par les cybercriminels.

COMMENT VOUS PROTÉGER FACE À CETTE MENACE ET COMMENT RÉAGIR EN CAS D'ATTAQUE ?

Découvrez tous nos conseils dans [notre fiche réflexe sur les rançongiciels](#)
cybermalveillance.gouv.fr

Infographie réalisée avec nos membres



Bitdefender