RANSOMWARE
MOBILE

DITES AU-REVOIR À VOS FICHIERS PERSONNELS

Ce type de logiciels tient en otage votre smartphone et les données qu'il contient en échange d'un prix à payer. Ce type de malware bloque l'écran de votre téléphone et vous empêche d'accéder aux fichiers ou aux fonctionnalités.

COMMENT CE MALWARE SE PROPAGE-T-IL?

Par la visite de sites web malveillants

En téléchargeant de fausses versions d'applis légitimes.

En cliquant sur des liens et des pièces jointes intégrées aux e-mails de phishing.

QUELS SONT LES RISQUES?

Il se peut que vous deviez réinitialiser votre appareil aux paramètres d'usine et que vous perdiez toutes vos données.

Un hacker peut accéder à toutes les données de votre smartphone, et partager vos données avec des tierces parties.

QUE FAIRE ?

Sauvegardez fréquemment vos données et assurez-vous que vos applis et votre système opérationnel sont mis à jour.

Évitez de télécharger des applis ne provenant pas de boutiques officielles.

Si possible, installez une appli de sécurité mobile qui vous avertira si votre smartphone est infecté.

Méfiez-vous d'e-mails ou de sites web suspects qui semblent trop beaux pour être vrais.

N'accordez pas de droits d'administrateurs à qui que ce soit.

Ne payez pas la rançon. Vous financeriez des criminels et les encourageriez à poursuivre leurs activités illégales.