KASPERSKY LAB

RANSOMWARE

Ces images pourraient coûter près de 300$
Il s'agit du montant moyen de la rançon demandé par un ransomware.

RANSOMWARES À CHIFFREMENT

Ils chiffrent les fichiers de façon à ce que les victimes ne puissent plus les utiliser. Si les utilisateurs veulent récupérer leurs fichiers, ils doivent payer la rançon.

VERROUILLEURS

Ils bloquent les ordinateurs des victimes de façon à ce que personne ne puisse utiliser son dispositif. Ce type de malware est en général plus facile à traiter que ceux à chiffrement.

CANAUX DE DISTRIBUTION

- Pièces jointes dans un e-mail
- Fichiers téléchargés sur Internet
- Liens malveillants
- Réseaux locaux

PLATEFORMES

EXTENSIONS DE FICHIERS DANGEREUSES*

EXE, DOC DOCX, XLS XLSX, PPT PPTX, VBS, JS, LNK, SCR

*Elles peuvent être dissimulées sous des formats ZIP ou RAR

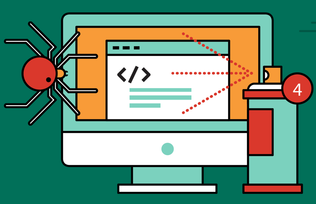
Déverrouillage iOS

Android

Internet des Objets (prochainement)

COMMENT S'EN PROTÉGER ?

1. N'ouvrez pas de pièces jointes suspicieuses dans un e-mail ni des fichiers téléchargés
2. Mettez à jour votre système d'exploitation et votre logiciel rapidement
3. Faites régulièrement des sauvegardes de tous les documents importants

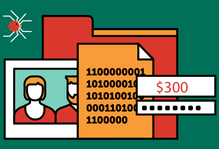


4. Installez Kaspersky Internet Security

Le module Surveillance du système contrôle les menaces en temps réel, les bloque et restaure les fichiers modifiés.

J'AI ÉTÉ INFECTÉ : QUE PUIS-JE FAIRE ?

RANSOMWARES À CHIFFREMENT



1. Désinfectez votre dispositif avec Kaspersky Internet Security
2. Restaurez les fichiers chiffrés grâce aux sauvegardes

ou

3. Utilisez les outils de déchiffrement sur noransom.kaspersky.com

ou

4. Payez la rançon (non recommandé)

VERROUILLEURS

Utilisez Kaspersky Windows Unlocker

KASPERSKY LAB

© 2016 AO Kaspersky Lab. Tous droits réservés.

Eur'Net - Kaspersky Gold Partner, Intégrateur Kaspersky depuis 1997, http://antivirus-france.com - 0415 63 00 00