



ANSSI

Agence nationale de la sécurité des systèmes d'information

ACTUALITÉS

NE SOYEZ PLUS OTAGE DES RANÇONGIÉELS !

Face à l'augmentation des attaques par rançongiciels à l'encontre de tout type de structure (administrations, entreprises, PME, professions libérales...), l'ANSSI propose, en collaboration avec la fédération Eben, de former aux réflexes à adopter. La plaquette « Alerte aux rançongiciels » informe donc sur les bonnes pratiques mais surtout sur les règles de bon sens à appliquer en cas d'urgence.

Un **rançongiciel** (ou cryptolocker) est un programme malveillant dont le but est de chiffrer partiellement ou entièrement les données d'un système. L'attaquant est de propose ensuite à la victime de récupérer ses données en échange du paiement d'une rançon (sans aucune garantie en la matière). Depuis plusieurs mois, l'ANSSI constate une recrudescence de ces attaques à qui visent sans discernement l'ensemble des acteurs économiques, de toute importance, mais également les particuliers.

« VOS DONNÉES EN OTAGE »

Alerte aux rançongiciels

Vos données en otage, contre de l'argent !

Vous êtes de plus en plus nombreux à recevoir des messages chiffrés avec des pièces jointes et/ou des liens qui sont piégés. NE CLIQUEZ PAS DESSUS !

Un virus pourrait chiffrer vos données et exiger une rançon. La police ne garantit pas la récupération de l'intégralité de vos données.

Il est constaté de plus en plus d'inscriptions par des emails qui contiennent des pièces jointes et/ou des liens piégés. Ces messages frauduleux sont maintenant plus difficiles à détecter par les utilisateurs car ils sont très souvent de parfaites copies, avec de vrais logos et sans fautes d'orthographe.

VOICI QUELQUES RÈGLES DE BON SENS QU'IL FAUT ABSOLUMENT RESPECTER :

Ces réflexes sont indispensables et peuvent sauver votre entreprise !

N'ouvrez pas les messages dont la provenance ou la forme est douteuse.
Apprenez à distinguer des emails piégés en deux minutes sur : <http://www.back-ucademy.fr/cambdats/wdly>

Effectuez des sauvegardes régulières de vos données.
Déplacez physiquement la sauvegarde de votre réseau et placez la en lieu sûr. N'ouvrez-elles avant qu'elle fonctionne.

Mettez à jour vos logiciels (utils, Windows, antivirus, Antispam, PME, navigateur, etc.).
Et si possible, déterminez les mises à jour hebdomadaires de tous vos logiciels qui permettent d'éliminer des tâches de manière automatique. Cette règle évite la propagation des rançongiciels et la vulnérabilité des applications.

Créer un compte « utilisateur » et n'utilisez que celui-ci, une fois votre ordinateur configuré.
Cette règle réduira l'impact de vos actions malveillantes.

Vous trouverez toutes les recommandations de l'ANSSI sur le site : www.ssi.gouv.fr
En complément, il est recommandé de prendre quotidiennement connaissance des bulletins d'alerte du CERT-FR : bulletins.cert-fr.fr
Le CERT-FR est à votre disposition pour vous assister dans vos actions informatiques sur ces sujets.

Pour pallier à cette situation l'ANSSI s'est associée à la **Fédération Eben** afin d'élaborer ce document de prévention à destination de tous, qui rappelle les réflexes indispensables à adopter pour ne plus rester vulnérable face aux rançongiciels.

Avec plus de 2 000 adhérents, la Fédération EBEN (Entreprises du Bureau et du Numérique) assure la représentation des distributeurs de fournitures de bureau, de systèmes d'impression, informatiques et télécoms... un public d'autant plus concerné par la sécurité du numérique. La plaquette répond à un besoin exprimé par la fédération en termes de sensibilisation et de prévention, mais intéressera plus généralement l'ensemble des organisations susceptibles d'être un jour touchées par un rançongiciel. Et comme souvent en matière de sécurité informatique, la prévention et la préparation restent les meilleurs atouts pour faire face à ces risques.

Un document à mettre entre toutes les mains pour la protection de vos données et de celles de votre entreprise. Et pour en savoir plus sur les rançongiciels, [consultez également le bulletin d'actualité du Cert-FR qui dresse un état des lieux de la menace.](#)

Télécharger [Alerte aux rançongiciels – Vos données en otage contre de l'argent](#)