RANÇONGICIEL : LES RECOMMANDATIONS DE SÉCURITÉ

Category: Sécurité informatique
Tag: Enquête

Message électronique douteux avec des pièces jointes ? Clé USB d'origine inconnue ?

Alors que se propage, depuis le 27 juin 2017, un programme informatique malveillant de type micrologiciel, l'Agence nationale de la sécurité des systèmes d'information (Anssi) fait un certain nombre de recommandations.Nous reproduisons un document publié sur le site service-public.fr qui est important. L'environnement Internet n'est pas composé que de gentilles personnes... Suivez bien les conseils donnés.

Il est notamment conseillé aux utilisateurs de :

- de ne pas ouvrir les pièces jointes des messages électroniques suspects (fautes d'orthographes, pièces jointes au nom trop succinct ou trop générique...) ;
- de se méfier de courriel de type « hameçonnage ciblé » qui personnalise le contenu par rapport à l'environnement de l'utilisateur afin de tromper sa vigilance ;
- de ne pas suivre les liens des messages électroniques suspects et de vérifier la cohérence entre l'adresse affichée dans le contenu et le lien effectif ;
- de ne pas réactiver des fonctionnalités désactivées dans la configuration des logiciels, même si le fichier ouvert y incite par un message particulier.

En cas d'incident :

- pensez à déconnecter immédiatement du réseau les équipements identifiés comme compromis ; alertez le responsable sécurité ou le service informatique au plus tôt ;
- sauvegardez les fichiers importants sur des supports amovibles isolés ;
- et ne payez pas la rançon.

Nous publions le document avec le lien car il mène vers d'autres informations : Rançongiciel : les recommandations de sécurité