

#1 Sécurité numérique

Publié le 25 avril 2018 – Mis à jour le 25 avril 2018



Sécurité numérique est une rubrique qui se compose d'articles visant à sensibiliser les différentes populations de l'UCA à la sécurité numérique

VIRUS SUR LES RÉSEAUX SOCIAUX !

Depuis quelques jours un virus se propage via les réseaux sociaux. En effet, nous constatons une augmentation du nombre d'alertes d'infections par le Ransomware Locky dans certains établissements. Ce virus crypte irréversiblement les données du poste infecté et celles accessibles en réseau. Il se diffuse au travers des images diffusées sur les réseaux sociaux, notamment Facebook et LinkedIn.

COMMENT NE PAS SE FAIRE PIÉGER ?

Le procédé est simple : lorsque vous naviguez sur les réseaux sociaux tel que Facebook ou LinkedIn de nombreuses photos apparaissent dans votre journal. Si vous cliquez dessus, dans certains cas, cela déclenche automatiquement un téléchargement du fichier. Ceci est suffisant pour télécharger le virus sur votre poste. Pour éviter de vous faire piéger voici quelques conseils :

- les réseaux sociaux affichent généralement le contenu d'une image avant de la télécharger alors si ce n'est pas le cas méfiez-vous.
- si vous cliquez sur une image et qu'un téléchargement de fichier survient automatiquement annulez le téléchargement et n'ouvrez pas le fichier en question
- cela concerne les fichiers images ou photo se terminant par les extensions .SVG, .JS et .HTA

Cette campagne d'infection baptisé "ImageGate" vise les ordinateurs sous Windows et entraîne le chiffrement des données du poste infecté. A l'heure actuelle les outils de défense habituels ne reconnaissent pas cette souche virale. Afin de se protéger suivez les conseils indiqués ci-dessus.

<https://dsi.uca.fr/securite-numerique/1-securite-numerique-1> (<https://dsi.uca.fr/securite-numerique/1-securite-numerique-1>)