Contrer les assauts de Locky

Le rançongiciel Locky, qui se propage par mail, frappe au hasard et fait des ravages.

Anticiper reste la meilleure des parades pour l'éviter.

Ce kidnappeur de données attaque sévèrement la France depuis la mi-février.

Locky. qui ne touche pour le moment que les PC sous Windows, pourrait bien obtenir la palme de la plus belle arnaque de la décennie.

La méthode de propagation est pourtant extrêmement classique. Une pièce jointe dans un courriel mentionnant ici une facture de l'0pérateur Free, là un reçu de paiement, ici encore un accusé de réception d'une commande faite sur le Net, est envoyée à tout va. On ouvre le fichier joint (.doc ou .pdf) et... c'est le drame.

Un petit programme se connecte au Web et rapatrie un logiciel malveillant qui chiffre les données de votre ordinateur (documents texte, PDF .images. etc.). Comprenez qu'elles deviennent illisibles. Plus moyen d‘y accéder, sauf peut-être à payer une rançon de un à quatre bitcoins (jusqu'à plus de 1500 euros au cours actuel) ! Et même ainsi, vous n’avez aucune assurance que la clé pour déverrouiller vos données vous sera fournie en retour. Jusqu'ici, aucun remède n’a été trouvé pour casser le chiffrement: de Locky. Alors autant tout mettre en œuvre pour qu’il ne fasse pas son nid dans votre PC.

COMMANDEHENT N°1

De cliquer sans réfléchir tu t'abstiendras

C’est ainsi que tout commence. Le courriel que vous avez sous les yeux vous semble-t-il normal ? Même si vous êtes client de Free Mobile,l’opérateur a-t-il pour habitude de vous envoyer une facture par mail ? Ce reçu d'une boutique en ligne est-i1 légitime sur cette adresse ? Vérifiez bien le mon de l'expéditeur (s’i1 s'agit de votre adresse mai1, jetez le courriel immédiatement). Restez vigilant sur tout ce qui vient d'inconnus.

COMMANDEMENT N°2

Le registre de Windows tu modifieras

C'est une parade assez efficace pour empêcher l'intrusion de Lucky (et uniquement lui, dans sa version actuelle). Pour s’installer, le rançongiciel doit créer une clé de registre. Si elle est déjà présente, le processus est stoppé net. Lancez *Regedit* en tapant son nom dans le champ de recherche de Windows. Déroulez la clé ***HKEY_CURRENT_USER***. Effectuez un clic droit sur ***SOFTWARE*** et choisissez ***Nouveau, Clé***. Saisissez le nom ***Locky*** et validez. Faites maintenant un clic droit sur la clé ***Locky*** fraichement créée puis activez ***Autorisations***. Dans la fenêtre qui s'affiche, sélectionnez ***Administrateur*** puis cochez les cases ***Refuser*** pour le ***Contrôle total et la lecture***. Validez et fermez le registre.

COMMANDEMENT N°3

Ton antivirus tu épauleras

Même si, à 1’heure actuelle, Locky passe encore à travers les mailles du filet de la plupart des antivirus, les éditeurs travaillent d’arrache-pied pour trouver comment bloquer son exécution. BitDefender vient tout juste de livrer un outil capable de bloquer les principaux rançongiciels actuels dont Locky. Installez-le sans tarder en vous rendant sur le site http://tinyurl.com/jyadeb9.

COMMANDEMENT N°4

L‘aperçu de documents tu utiliseras

Vous avez un doute concernant un fichier Word ou PDF joint à un mail ?

Ne double-cliquez pas dessus pour qu’il s’ouvre avec Word ou Acrobat Reader. Déplacez-le sur le Bureau et observez sa prévisualisation dans une fenêtre de l’Explorateur de fichiers de Windows (***Alt + P*** pour obtenir l’aperçu). Si rien ne s'affiche, passez votre chemin.

COMMANDEMENT N°5

Des sauvegardes régulières tu effectueras

Dans le cas des rançongiciels, mieux vaut multiplier les précautions.

Aussi, procédez régulièrement et manuellement à des sauvegardes des données de votre machine ou même de l’intégralité du disque dur.

Attention, le chiffrement peut aussi s’appliquer aux disques connectés et aux disques réseau

(NAB).

FABRICE BROCHAIN