Sécurité économique territoriale
Rhône-Alpes

MESSAGE D'ATTENTION
- VIRUS RANÇON -

Très récemment, un salarié d'une entreprise implantée dans le sud de la région Rhône-Alpes ouvre une pièce jointe nommée « *scan.zip* » contenue dans un courriel. Immédiatement après, l'ensemble des répertoires de fichiers utilisés dans la journée ont été encryptés et rendus inutilisables.

Une seconde pièce jointe au mail contenait les instructions à suivre pour payer une « *rançon* » afin d'obtenir la clé de déchiffrement.

DE QUOI PARLE-T-ON ?

Un ransomware (*en français rançongiciel, crypto-virus ou virus rançon*), est un logiciel malveillant pouvant entraîner soit le blocage d'un ordinateur, soit le chiffrement des données qu'il renferme, ou encore la récupération d'informations sensibles.

Transmis par messagerie, le courriel contient généralement une pièce jointe au format « *.pdf* », « *.zip* », ou « *.exe* » qu'on vous demande d'ouvrir. Un document ne contenant aucune information intéressante pour le destinataire s'ouvre et un virus ou un cheval de Troie s'installe alors automatiquement sur l'ordinateur à l'insu de l'utilisateur.

A noter que ces fichiers malveillants peuvent également être intégrés directement dans des pages web ou diffusés via des liens ou des films présents sur les réseaux sociaux tels que Facebook, Netlog, Google+, etc.

Apparu fin 2013, le virus *cryptolocker*, une nouvelle variante de ransomware, a pour effet de chiffrer les fichiers de l'utilisateur, les rendant inutilisables et menaçant de les supprimer si une rançon n'est pas versée à l'issue du compte à rebours affiché à l'écran.

Payer se révèle souvent sans aucun effet car une fois la rançon réglée, le cybercriminel disparaît sans transmettre la clé de déchiffrement nécessaire au déblocage.

QUE FAIRE ?

En amont : *Sensibiliser régulièrement* les salariés et ce quel que soit le niveau de responsabilité exercé. Tout personnel connecté au réseau de l'entreprise est susceptible d'être rendu destinataire de mails piégés pouvant infecter au mieux son ordinateur et au pire l'intégralité du système d'information de l'entreprise.

***Effectuer des sauvegardes régulières* de l'ensemble du système informatique et des données contenues. S'assurer régulièrement de leur viabilité.**

***Installer et mettre à jour régulièrement* antivirus et firewall.**

En cas de problème : *Prendre en photo* tous les écrans (*mail frauduleux et ses pièces jointes*) et noter toutes les actions réalisées ainsi que les heures

Il est possible d'éradiquer le virus en démarrant le PC sur un antivirus au boot préalablement chargé sur un CD ou une clé USB. L'ordinateur sera auparavant paramétré pour redémarrer via ce support amovible en lieu et place du système interne.

De nombreux sites traitant de la décontamination des ransomwares sont facilement consultables sur internet.

***Une veille régulière* permettra d'anticiper et de s'adapter aux nouvelles menaces.**

En cas de problème avéré ou de simple tentative :

***Déposer rapidement plainte* auprès du service de police ou de gendarmerie territorialement compétent.**

Lettre électronique éditée par la région de gendarmerie de Rhône-Alpes – 36 bd de l'Ouest – 69580 Sathonay-Camp - ☎: 04.37.85.21.00
Rédaction : Cellule Intelligence Économique régionale