Sécurité économique territoriale
Rhône-Alpes

MESSAGE D'ATTENTION
VIRUS RANÇON « CTB LOCKER »

Depuis le début du mois de février 2015, une nouvelle campagne d'attaques informatiques de type « *ransomware CTB locker* » cible les entreprises française.

En Rhône-Alpes, une des sociétés touchées a constaté le cryptage de plus de 250 000 fichiers de tous types.

Cet incident a engendré un important manque à gagner, une perte de données irréversible et des dysfonctionnements dans tous ses services.

Un ransomware ou virus rançon est un logiciel malveillant cryptant les données des machines qu'il infecte et ordonnant le paiement d'une rançon *(souvent en monnaie virtuelle – Bitcoins)* **pour en restaurer l'accès. La nouvelle version du virus « *CTB Locker* » réussit à passer outre les firewalls et antivirus les plus sophistiqués, si ceux-ci sont mal configurés.**

« *CTB Locker* » se propage essentiellement via des courriels d'apparence anodine, personnalisés au maximum (*notamment grâce à des informations recueillies par le biais des techniques dites de social engineering*) **en vue de ne pas éveiller les soupçons des utilisateurs ciblés. Un document, identifié comme étant une facture, une plainte de client, un bon de commande, …, comportant l'extension « *.cab* » (***format de fichier Microsoft compressé***) contient l'exécutable malveillant, lequel s'installe une fois le document ouvert puis crypte les données à l'insu de l'utilisateur. Peu de temps après, une fenêtre « *pop up* » apparaît et *informe le salarié de l'attaque* dont il vient d'être victime et de la nécessité de *payer une rançon* avant l'échéance d'un *compte à rebours* affiché à l'écran pour obtenir un retour à la normale (*Cf copie d'écran ci-dessus*).**

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.

En amont :

- *Sensibiliser régulièrement* les salariés et ce quel que soit le niveau de responsabilité exercé. Tout personnel connecté au réseau de l'entreprise peut recevoir un mail piégé pouvant infecter au mieux son ordinateur et au pire l'intégralité du système d'information.

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

- *Bloquer* les extensions « *.cab* » dans les applications messagerie,

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

- *Mettre en place une veille régulière* pour anticiper et s'adapter aux nouvelles menaces.

En cas d'attaque :

- *Prendre en photo les écrans ou réaliser des copies d'écran* (*mail frauduleux et ses pièces jointes*) et *noter* l'ensemble des *actions réalisées.*

- *Isoler* les serveurs et l*ancer* un scan antivirus,

- *Identifier* l'adresse IP émettrice du mail,

- *Supprimer* le profil utilisateur problématique sur les serveurs,

- *Supprimer* l'ensemble des fichiers cryptés,

- *Restaurer* l'ensemble des dossiers et fichiers depuis des *sauvegardes* ou des *points de restauration* système réalisés antérieurement à l'attaque,

- *Communiquer* immédiatement sur l'attaque auprès de tous les utilisateurs,

- *Analyser* en vue de comprendre les raisons pour lesquelles le mail n'a pas été filtré par les systèmes de sécurité.

Dans tous les cas, il vous faudra procéder avec minutie au risque de perdre vos fichiers.

En cas de problème avéré ou de simple tentative : *Déposer rapidement plainte* auprès du service de police ou de gendarmerie territorialement compétent.

Lettre électronique N° 05 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