Sécurité économique territoriale

Rhône-Alpes

Alerte

MESSAGE D'ATTENTION

RANSOMWARE « LOCKY »

Récemment, une entreprise rhonalpine a reçu un mail ayant pour objet « ***Proforma Invoice*** », dont le texte est rédigé dans un français approximatif, contenant une pièce jointe dénommée « ***facture (suivi de 5 chiffres).doc*** », pouvant laisser supposer qu'il s'agit d'une confirmation de commande.
Suspicieux et ce à juste titre, le chef d'entreprise n'a pas ouvert le document et a immédiatement alerté l'ensemble des salariés de son groupe.
Grand bien lui en a pris puisqu'après analyses, il s'avère que ce courriel contenait un ransomware dénommé ***LOCKY***. Cette excellente réaction a vraisemblablement permis d'éviter le pire.

DE QUOI PARLE-T-ON ?

Similaire au trojan Dridex (*cf message d'attention N° 8*), le virus Locky est un crypto-ransomware chiffrant les documents contenus dans un ordinateur en vue de rendre impossible leur ouverture. Depuis la mi-février 2016, Locky est transmis par le biais d'une campagne mondiale de courriels malicieux contenant des pièces jointes Invoice au format Word « ***.doc*** ».

Des fichiers de type « ***.zip*** » contenant des fichiers javascript peuvent également accompagner ces pourriels. Eu égard à son ampleur, cette action pourrait être l'œuvre d'un groupe cybercriminel très bien organisé.

Une fois la pièce jointe ouverte, une macro s'exécute automatiquement, permettant ainsi le téléchargement et l'installation du ransomware. Les fichiers de l'ordinateur et des périphériques USB branchés (*clé USB, disque dur externe, ...*) sont alors chiffrés et leur extension modifiée en « ***.locky*** ». Par la suite, le fond d'écran est automatiquement modifié et un fichier « ***locky_recover_instructions.txt*** » contenant les instructions de paiement s'ouvre. La rançon exigée devra être réglée en bitcoins (*monnaie électronique, 1 bitcoin équivalant à environ 390 €*). Pour l'heure, il semblerait qu'aucune solution ne permette de récupérer les documents chiffrés.

QUE FAIRE ?

Bien que classique, cette campagne de ransomware mise une nouvelle fois sur la méconnaissance des utilisateurs et leur manque de vigilance. Les potentielles victimes peuvent toutefois facilement éviter de tomber dans le piège en appliquant quelques ***mesures de bon sens***.

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.

Règle : Tout mail de provenance douteuse doit aussitôt être supprimé sans être ouvert.

- ***Effectuer des sauvegardes régulières*** de l'ensemble du système informatique et des données contenues. S'assurer régulièrement de leur viabilité.
- ***Désactiver les macros exécutables*** automatiquement dans Microsoft Word et Excel. Pour vous aider, consulter le ticket Microsoft suivant :

https://support.office.com/fr-be/article/Activer-ou-désactiver-les-macros-dans-les-documents-Office-7b4fdd2e-174f-47e2-9611-9efe4f860b12?ui=fr-FR&rs=fr-BE&ad=BE

- ***Installer et mettre à jour régulièrement*** antivirus, antimalware et firewall.
- ***Mettre en place une veille*** pour anticiper et s'adapter aux nouvelles menaces.

(***Exemples de sites*** ***: http://www.ssi.gouv.fr/, http://cert.ssi.gouv.fr/, http://www.malekal.com/, ...***).

En cas d'attaque :

- Dans le cas où la pièce jointe aurait été ouverte, ***isoler immédiatement l'ordinateur*** compromis en le déconnectant du réseau. **L'objectif est de bloquer la poursuite du chiffrement et la destruction des dossiers partagés**.
- ***Prendre en photo les écrans ou réaliser des copies d'écran*** (*mail frauduleux et ses pièces jointes*) et noter l'ensemble des actions réalisées.
- ***Contacter rapidement*** le responsable informatique ou la société de maintenance.
- ***Communiquer*** immédiatement sur l'attaque auprès de l'ensemble des utilisateurs.

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° 10 – Février 2016** éditée par la région de gendarmerie de Rhône-Alpes – 36 bd de l'Ouest – 69580 Sathonay-Camp - ☎: 04.37.85.21.15
Rédaction : Cellule Intelligence Économique régionale