Sécurité économique territoriale

Auvergne - Rhône-Alpes

MESSAGE D'ATTENTION

ATTAQUE RANSOMWARE SUR SERVEUR

DE QUOI PARLE T-ON ?

Dernièrement, une société rhônalpine a été victime d'une attaque par ransomware (lo*giciel rançonneur*) de type « *.pedant* », une variante issue de la famille Matrix.

Si ce phénomène n'a rien d'inédit, le mode d'attaque quant à lui semble avoir subi une évolution notable qui doit inquiéter. Jusqu'à présent ce type d'atteinte était essentiellement le fruit de campagne de mails avec liens ou pièces jointes infectées.

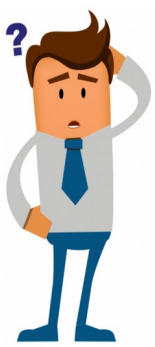
Dans le cas présent, il est établi que le serveur de la société a été directement ciblé. L'attaquant est parvenu à s'y introduire après avoir scanné ses ports. Une fois la faille décelée (*port(s) ouvert(s) vers l'extérieur*), il a pu prendre la main sur la machine, désactiver l'antivirus, changer les mots de passe et procéder au chiffrement des données.

L'intervention rapide de l'informaticien a toutefois permis de limiter les dégâts.

A l'instar des attaques classiques, le ransomware a introduit dans le système un fichier contenant les instructions pour un paiement en bitcoins, monnaie virtuelle décentralisée (*utilisateur difficilement identifiable*).

Si aucune somme n'a clairement été évoquée, celle-ci devait s'élever à plusieurs centaines voire plusieurs milliers d'euros.

QUE FAIRE ?



- ***Effectuer quotidiennement la sauvegarde des données sur des supports isolés du réseau*.** En ***vérifier périodiquement la viabilité*** par le biais ***de tests de restauration, même partiels***.
- ***Mettre à jour*** vos systèmes d'exploitation, logiciels, solutions de sécurité et applications.
- ***Installer des solutions de sécurité*** (*anti-virus, anti-spams, firewall, ...*) sur les postes de travail et sur le serveur de l'entreprise.
- ***Ne pas ouvrir les pièces jointes ou liens contenus*** dans des courriels dont l'expéditeur est inconnu.
- ***Sensibiliser régulièrement*** l'ensemble des salariés aux problématiques de sécurité informatique.
- ***Ne pas naviguer sur internet*** via le réseau de l'entreprise depuis un compte ayant des privilèges « ***Administrateur*** ». La création de comptes « ***utilisateurs*** » est primordiale.
- ***Utiliser des mots de passe forts***, et les ***changer régulièrement*** (2 à 3 fois par an).

EN CAS D'ATTAQUE...

- ***Isoler immédiatement la machine*** compromise en la déconnectant du réseau (*arrêt du Wi-Fi, câble Ethernet débranché ; l'objectif étant de bloquer la propagation du chiffrement et la destruction des dossiers partagés*).
- ***Prendre en photo les écrans*** et ***noter*** l'ensemble des actions réalisées.
- ***Contacter rapidement le responsable informatique*** ou la société de maintenance. Vérifier l'intégralité du réseau, d'autres machines ayant pu être infectées. Désinfection des postes et restauration des données (*si vous avez préalablement effectué des sauvegardes bien sûr*).
- ***Changer*** l'ensemble des ***mots de passe*** (*serveur et ordinateurs*) et ***verrouiller l'ensemble des ports du serveur***.
- ***Ne jamais payer la rançon*** exigée.
- ***Communiquer immédiatement sur l'attaque*** auprès de l'ensemble des utilisateurs.
- ***Déposer plainte*** auprès du service de gendarmerie ou de police territorialement compétent.
- ***Prévenir votre assurance*** pour éventuellement mettre en route la procédure d'indemnisation dans le cas où un contrat "***perte d'exploitation***" ou "***risques cyber***" aurait été souscrit.

Seule une sauvegarde quotidienne et viable permet de surmonter sereinement ce type d'attaque

Lettre électronique N° 24 – 20 Février 2019 - éditée par la région de gendarmerie de Rhône-Alpes – 36 bd de l'Ouest – 69580 Sathonay-Camp : 04.37.85.21.15
Rédaction : Cellule Sécurité Économique régionale