Sécurité économique territoriale
Auvergne - Rhône-Alpes

MESSAGE D'ATTENTION

ATTAQUE RANSOMWARE SUR SERVEUR

DE QUOI PARLE T-ON ?

Dernièrement, de nombreuses entreprises et institutions territoriales rhônalpines ont été victimes d'une attaque par ransomware (*logiciel rançonneur*) de type « *SODINOKIBI*», une variante issue de la famille « *GRANDCRAB* ».
Si ce phénomène n'a rien d'inédit, le mode d'attaque quant à lui doit inquiéter. Jusqu'à présent ce type d'atteinte était essentiellement le fruit de campagnes de mails avec liens ou pièces jointes infectées.
Dans le cas présent, il est établi que les serveurs des entités touchées ont été directement ciblés. L'attaquant est parvenu à s'y introduire après avoir scanné les ports ouverts. Une fois la faille décelée (*port ouvert + faille du logiciel de supervision KASEYA*), il a pu procéder au chiffrement des données. L'intervention rapide des informaticiens a toutefois permis de limiter les dégâts mais certaines sociétés ayant leurs sauvegardes non externalisées (*et qui ont été chiffrées lors de l'attaque*) ont vu leurs activités fortement impactées.
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 intraçable. En vue d'obtenir la clé de déchiffrement, les victimes doivent débourser des sommes comprises entre 640 000 et 700 000 dollars américains.

QUE FAIRE ?

- ***Effectuer quotidiennement la sauvegarde des données sur des supports isolés du réseau*.**
- ***Externaliser les sauvegardes seraient la solution idéale*.** En ***vérifier périodiquement la viabilité*** par le biais ***de tests de restauration, même partiels***.
- ***Si vous êtes équipé de l'outil de supervision KASEYA****, le désinstaller de toutes vos machines s'il ne sert plus, sinon, appliquer les mises à jour.*
- ***Demander au service informatique de fermer les ports du serveurs*** non nécessaires à son bon *fonctionnement.*
- ***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(s) serveur(s) 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 "***risques cyber***" aurait été souscrit.

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

Lettre électronique N° 27 – 20 janvier 2020 - 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