Gendarmerie nationale
MINISTÈRE DE L'INTERIEUR

LUTTE CONTRE LES RANCONGICIELS

Depuis plusieurs mois les systèmes informatiques des entreprises, administrations et même des particuliers font l'objet d'attaques cyber visant extorquer de l'argent aux propriétaires des machines infectées. Cette technique appelée ransomware ou rançongiciel, peuvent provoquer de graves troubles aux systèmes infectés, parfois jusqu'à la destruction des données informatiques.

DEFINITION *:*

Un rançongiciel (de l'anglais ransomware ou logiciel rançon, est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. Un ransomware peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent .

MODE D'INFECTION D'UN RANCONGICIEL :

La machine peut être infectée après l'ouverture d'une pièce-jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en navigant sur des sites compromis, ou encore suite à une intrusion dans le système. Les données sont alors cryptées empêchant le propriétaire de la machine infecté ou le réseau de fonctionner.

GROUPEMENT DE GENDARMERIE DÉPARTEMENTALE DE LA DRÔME
Maison de l'Armée Avenue Dupré de Loire 26 000 VALENCE Tel : 04 75 82 52 00

COMMENT SE PROTEGER :

1) *Pour se prémunir d'un ransomware, effectuez des sauvegardes régulières de vos données C'est le meilleur moyen de couper l'herbe sous le pied aux pirates souhaitant prendre vos données en otage ! Déplacez physiquement la sauvegarde de votre réseau (hors réseau), placez-la en lieu sûr et veillez à ce qu'elle fonctionne !*

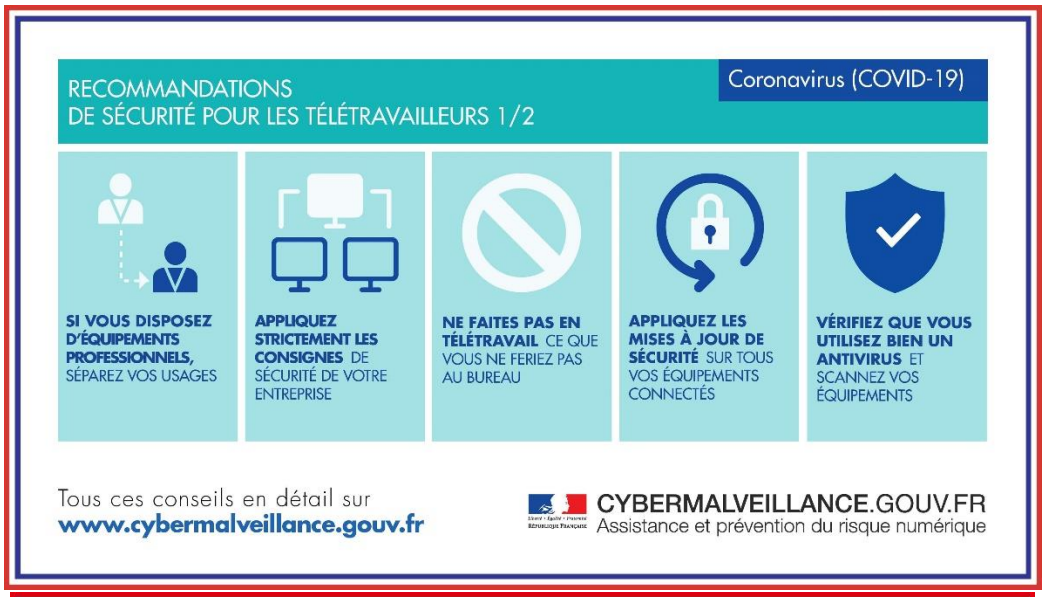
2) *N'ouvrez pas les messages dont la provenance ou la forme est douteuse, il pourrait s'agir d'un rançongiciel Ne vous laissez pas tromper par un simple logo ! Pire, le hacker peut avoir récupéré certaines de vos données préalablement (les noms de vos clients par exemple) et créer des adresses de messagerie ressemblant à un détail près à celle de vos interlocuteurs habituels. Restez donc très vigilants ! Certains messages paraissent tout à fait originaux.*

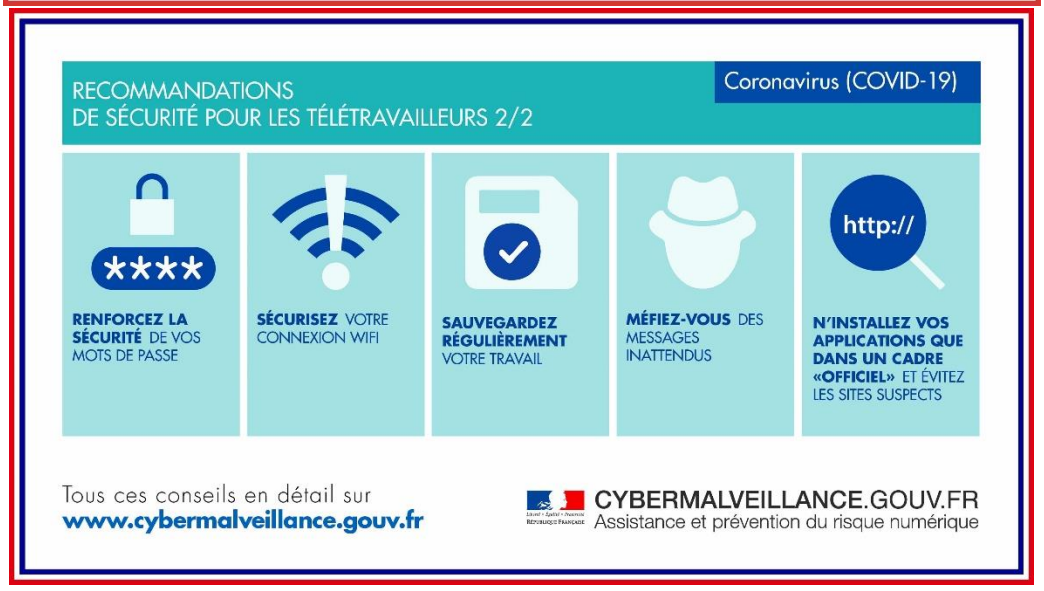
3) *Pour se prémunir d'un ransomware, apprenez à identifier les extensions des fichiers douteuses Vous recevez habituellement des fichiers en .doc ou .mp4 (par exemple) et le fichier du message dont vous avez un doute se finit par un autre type d'extension ? Ne les ouvrez surtout pas ! Exemples : pif ; .com ; .bat ; .exe ; .vbs ; .lnk… Attention à l'ouverture de pièces jointes de type .scr ou .cab. Téléchargez vos logiciels uniquement sur des sites de confiances, efiez vous des contrefaçons.*

4) *Pour se prémunir d'un ransomware, mettez à jour vos principaux outils On ne vous le dira jamais assez : Windows, antivirus, lecteur PDF, navigateur… Veillez à leurs mises à jour ! Si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera en effet la propagation des rançongiciels via les vulnérabilités des applications. Considérez que, d'une manière générale, les systèmes d'exploitation en fin de vie, qui ne sont plus mis à jour, donnent aux attaquants un moyen d'accès plus facile à vos systèmes.*

5) *Pour se prémunir d'un ransomware, utilisez un compte « utilisateur » plutôt qu' « administrateur » Ne naviguez pas depuis un compte administrateur. L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur. Préférez l'utilisation d'un compte utilisateur. Cela ralentira, voire dissuadera le voleur dans ses actions malveillantes.*

LES RISQUES LIES AU TELETRAVAIL :





GROUPEMENT DE GENDARMERIE DÉPARTEMENTALE DE LA DRÔME
Maison de l'Armée Avenue Dupré de Loire 26 000 VALENCE Tel : 04 75 82 52 00


RECOMMANDATIONS DE SÉCURITÉ
LIÉES AU TÉLÉTRAVAIL POUR LES EMPLOYEURS 1/2
Coronavirus (COVID-19)
123456
ÉQUIPEZ VOS COLLABORATEURS DE MOYENS MAÎTRISÉS
FILTREZ ET CLOISONNEZ VOS ACCÈS EXTÉRIEURS
SÉCURISEZ VOS ACCÈS EXTÉRIEURS (VPN, 2FA...)
RENFORCEZ VOTRE POLITIQUE DE GESTION DE MOTS DE PASSE
AYEZ UNE POLITIQUE STRICTE DE DÉPLOIEMENT DES MISES À JOUR DE SÉCURITÉ
DURCISSEZ LES SAUVEGARDES DE VOS DONNÉES
Tous ces conseils en détail sur
www.cybermalveillance.gouv.fr
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique


RECOMMANDATIONS DE SÉCURITÉ
LIÉES AU TÉLÉTRAVAIL POUR LES EMPLOYEURS 2/2
Coronavirus (COVID-19)
UTILISEZ DES SOLUTIONS ANTIVIRALES PROFESSIONNELLES
JOURNALISEZ L'ACTIVITÉ DE VOS ÉQUIPEMENTS
SUPERVISEZ L'ACTIVITÉ DE VOS ACCÈS EXTERNES ET SYSTÈMES SENSIBLES
SENSIBILISEZ ET APPORTEZ UN SOUTIEN RÉACTIF À VOS COLLABORATEURS EN TÉLÉTRAVAIL
PRÉPAREZ-VOUS À AFFRONTER UNE CYBERATTAQUE
DIRIGEANTS : IMPLIQUEZ-VOUS ET MONTREZ L'EXEMPLE !
Tous ces conseils en détail sur
www.cybermalveillance.gouv.fr
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

QUE FAIRE EN CAS D'INFECTION PAR UN RANCONGICIEL :

1 Comment réagir ?

1- N'éteignez pas la machine concernée

L'interruption du processus de chiffrement empêche toute tentative ultérieure de récupération des données.

Mettez la machine en veille prolongée si possible.

2- Déconnectez immédiatement du réseau les machines concernées

L'objectif est de limiter la propagation de l'attaque en bloquant la poursuite du chiffrement des documents sur le réseau. Ne connectez pas non plus d'appareil supplémentaire sur le réseau.

3- Contactez immédiatement votre service informatique ou un expert

Vous êtes un ministère, un opérateur d'importance vitale (OIV), un opérateur de service essentiel (OSE) ou un fournisseur de service numérique (FSN) ?

→ Prévenez l'ANSSI :
www.ssi.gouv.fr/en-cas-dincident/

Vous êtes une collectivité territoriale, une entreprise privée (non OIV, non OSE), une association ?

→ Contactez si besoin cybermalveillance :
www.cybermalveillance.gouv.fr

5- Portez plainte auprès des services compétents

Pensez à réunir toutes les traces et indices qui pourraient servir comme éléments de preuve (ex : copies physiques de disques durs des postes compromis).

6- Identifiez la source de l'infection

Prenez les mesures nécessaire pour que la source de l'infection ne puisse pas être utilisée à nouveau (par l'application d'un correctif de sécurité par exemple).

GROUPEMENT DE GENDARMERIE DÉPARTEMENTALE DE LA DRÔME
Maison de l'Armée Avenue Dupré de Loire 26 000 VALENCE Tel : 04 75 82 52 00