RANCONGICIEL ou RANSOMWARE

CENTRE CYBER DU PACIFIQUE

EN BREF

QU'EST-CE QUE C'EST ?

Un ransomware (ou rançongiciel en français) est un type de logiciel malveillant qui prend en otage les fichiers d'un utilisateur ou d'une entreprise en les chiffrant, rendant ainsi les données inaccessibles. Ensuite, les cybercriminels demandent une rançon en échange de la clé de déchiffrement pour restaurer l'accès aux fichiers.
Le paiement de la rançon est souvent exigé en cryptomonnaie (comme le Bitcoin) pour anonymiser les transactions.

Le ransomware est un délit. Cela peut être un accès frauduleux à un système informatique (article 323-1 du Code pénal), une entrave au fonctionnement d'un système informatique (article 323-2 du code pénal), une modification suppression ou altération des données (article 323-3 du Code pénal), une extorsion ou du chantage (article 312-1 du Code pénal) ou une destruction des données (article 323-3-1 du Code pénal).

QUE FAIRE ?

1. Il est déconseillé de payer la rançon
2. Déconnectez votre appareil
3. Conservez les preuves
4. Identifiez le type de ransomware
5. Consultez un expert
6. Restaurez les données
7. Signalez l'incident aux autorités

▶ Voir détail page "Que faire"

COMMENT S'EN PROTEGER ?

- Sauvegardez régulièrement vos données
- Maintenez vos logiciels à jour
- Utilisez un logiciel antivirus et un pare-feu
- Évitez de cliquer sur des liens ou des pièces jointes suspectes
- Limitez les privilèges d'accès
- Désactivez les macros dans les documents

▶ Voir détail page "comment s'en proteger"

RANÇONGICIEL ou RANSOMWARE

CENTRE CYBER DU PACIFIQUE

QUE FAIRE ?

SI VOUS ÊTES VICTIME D'UN RANSOMWARE, VOICI LES ÉTAPES À SUIVRE :

Il est déconseillé de payer la rançon. Déjà parce qu'il n'y a aucune garantie que les criminels vous fournissent la clé de déchiffrement après paiement. De plus, cela encourage les attaques futures.

1. DÉCONNECTEZ VOTRE APPAREIL DU RÉSEAU

Coupez immédiatement la connexion à Internet (Wi-Fi, Ethernet) pour éviter que le ransomware ne se propage à d'autres appareils ou systèmes sur le réseau.

2. CONSERVEZ OU FAITES CONSERVER LES PREUVES PAR UN PROFESSIONNEL

Notamment ; un exemple de message piégé, les fichiers de journalisation (logs) de votre pare-feu, des copies physiques des postes ou serveurs touchés, pourront vous servir pour signaler cette attaque aux autorités et qui seront des éléments d'investigation.

3. IDENTIFIEZ LE TYPE DE RANSOMWARE

Si possible, notez les détails affichés par le ransomware (nom, adresse Bitcoin, etc.) pour identifier le type exact de malware. Des outils comme *ID Ransomware* peuvent vous aider à l'identifier.

4. CONSULTEZ UN PRESTATAIRE EXPERT EN CYBERSÉCURITÉ

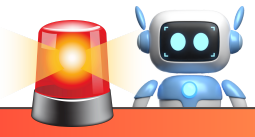
Il est essentiel de faire appel à des professionnels pour évaluer la situation et vérifier si une solution de déchiffrement existe déjà. Plusieurs ransomwares ont déjà des outils de déchiffrement gratuits disponibles en ligne, comme ceux fournis par *No More Ransom.*

5. RESTAUREZ À PARTIR DE SAUVEGARDES

Si vous avez des sauvegardes de vos données, vous pouvez effacer le système infecté et restaurer vos fichiers. Assurez-vous de nettoyer d'abord le système pour éliminer tout malware.

6. SIGNALEZ L'INCIDENT AUX AUTORITÉS

Portez plainte à la police ou la gendarmerie (Vos droits).
Informez des organismes spécialisés dans la cybersécurité, comme l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ou Cybermalveillance.gouv.fr



UNE MENACE SÉRIEUSE

Les ransomwares sont une menace sérieuse en Nouvelle-Calédonie, mais en adoptant des mesures de prévention solides, en sauvegardant régulièrement vos données, et en réagissant rapidement en cas d'infection, vous pouvez réduire considérablement les risques et les conséquences d'une attaque.

RANÇONGICIEL ou RANSOMWARE

CENTRE CYBER DU PACIFIQUE

COMMENT S'EN PROTÉGER ?

Sauvegardez régulièrement vos données :

Effectuez des sauvegardes fréquentes de vos fichiers importants sur un support externe ou un cloud sécurisé. Assurez-vous que les sauvegardes ne sont pas connectées en permanence à votre réseau pour éviter qu'elles ne soient également affectées en cas d'attaque.

Maintenez vos logiciels à jour :

Installez les mises à jour de sécurité pour votre système d'exploitation, vos logiciels et vos applications. Les mises à jour corrigent souvent des vulnérabilités que les ransomwares exploitent pour s'infiltrer.

Utilisez un logiciel antivirus et un pare-feu :

Un bon logiciel de sécurité peut détecter et bloquer les ransomwares avant qu'ils n'infectent votre système. Assurez-vous que votre antivirus est toujours à jour et qu'un pare-feu est activé.

Évitez de cliquer sur des liens ou des pièces jointes suspectes :

Soyez vigilant avec les emails non sollicités, surtout ceux avec pièces jointes ou liens. Vérifiez l'expéditeur et méfiez-vous des demandes d'informations confidentielles ou d'actions urgentes. Évitez les sites non sûrs, comme ceux de streaming ou hébergeant du contenu illicite.

Limitez les privilèges d'accès :

Réduisez les permissions des utilisateurs dans votre réseau, de sorte que seuls les utilisateurs autorisés puissent installer des programmes ou accéder à certaines données sensibles.

Désactivez les macros dans les documents :

Les ransomwares se propagent parfois par des documents Word ou Excel contenant des macros malveillantes. Désactivez les macros par défaut et activez-les uniquement pour des documents de sources fiables.

QUEL EST LE PROCÉDÉ ?

LES RANSOMWARES PEUVENT ÊTRE TRANSMIS PAR :

- Des emails piégés contenant des pièces jointes malveillantes ou des liens vers des sites infectés.
- Des failles de sécurité dans les logiciels ou systèmes d'exploitation.
- Des publicités malveillantes ou des sites web compromis.

IL EXISTE PLUSIEURS TYPES DE RANSOMWARES, DONT LES DEUX PRINCIPAUX SONT :

- Ransomwares de chiffrement : Ils chiffrent les fichiers et exigent une rançon pour la clé de déchiffrement.
- Ransomwares d'écran : Ils bloquent l'écran de l'ordinateur en affichant une fausse demande de rançon.