PRÉFET
DE LA LOIRE-ATLANTIQUE
Liberté
Égalité
Fraternité

Fiche action n°XX - Risque cyber (rançongiciel)

Définition

Un rançongiciel est un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. Lors d'une attaque par rançongiciel, l'attaquant met l'ordinateur ou le système d'information de la victime hors d'état de fonctionner de manière réversible.

Cela peut se matérialiser par :

- La présence d'un message de demande de rançon sous la forme de fichiers textes placés dans les répertoires
- L'inaccessibilité des fichiers.
- Le changement des extensions de fichier
- Le comportement anormal des applications
- Une exfiltration de données
- …

L'attaquant adresse alors un message non chiffré à la victime où il lui propose, contre le paiement d'une rançon, de lui fournir le moyen de déchiffrer ses données.

Actions à mener : mesures d'urgence

1. **Limiter l'impact** de l'incident en isolant le ou les matériels infectés :
   - Ne pas éteindre les machines infectées. *Même si cela parait contre-intuitif, le redémarrage de l'appareil peut aggraver la situation et/ou supprimer des indices et preuves pour l'investigation. Il faut cependant isoler les machines d'Internet et du réseau informatique.* Pour cela débrancher le câble Ethernet de l'ordinateur ou du serveur, ou bien désactiver la connexion Wi-Fi de l'appareil (se référer à la fiche pratique n°1).
   - Ne pas allumer les machines qui seraient éteintes avant l'attaque (sous peine de les infecter).
   - Vérifier que les sauvegardes sont bien isolées (si ce n'est pas le cas, les débrancher)
   - Couper internet via la box ou le cœur de réseau.

   Isoler d'internet le système d'information a généralement des impacts majeurs sur son fonctionnement et les services métiers. Il est préférable d'avoir au préalable établi cette procédure en heures ouvrées et non ouvrées (qui valide, qui procède à l'opération technique).

2. **Contacter une assistance spécialisée :**
   - Alerter immédiatement le service informatique
   - Contacter la cyber assurance ou le prestataire de réponse à incident (coordonnées à insérer si la commune en dispose)
   - Contacter « Pays de la Loire Cyber Assistance » au 0800 100 200 ou aller sur le site https://www.cybermalveillance.gouv.fr/, si pas de prestataire de réponse à incident

3. **Communiquer** auprès des parties prenantes :
   - Les administrés pour les informer de la continuité des services
   - Les agents pour les consignes à suivre
   - La CNIL s'il y a violation de données à caractère personnel,
   - La presse (il est préférable d'avoir identifié une personne en charge de la communication externe)

- La trésorerie / DGFIP
- La préfecture
- Le CERT-FR (obligatoire pour les plus grandes collectivités à partir de fin 2024)

4. **Porter plainte :**
   En parallèle de la résolution technique de l'incident, déposer plainte au commissariat de police ou à la brigade de gendarmerie dont dépend la commune

5. **Ne pas payer** la rançon :
   Même si le montant de la rançon parait accessible, rien n'assure, une fois la rançon payée, que les fichiers seront déchiffrés ou que l'ordinateur sera de nouveau accessible. De plus, cela peut consister à alimenter un système et démarrer un cercle vicieux : après avoir payé, la commune risque d'être identifiée comme « bon payeur » par les cybercriminels.

Actions à mener : mesures de reprise

6. **Mettre en place des solutions de contournement provisoires**
   Tant que les investigations et la remédiation n'ont pas abouti, il est risqué de remettre en production le système d'information. Il est préférable d'avoir prévu des systèmes alternatifs et provisoires afin de fournir quelques services essentiels à la gestion de crise (téléphones avec partages de connexion, postes informatiques isolés avec imprimantes directement connectées, messagerie externalisée provisoire…)

7. **Procéder à l'investigation**
   A l'aide d'un prestataire, identifier la source de l'infection et prendre les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

8. **Faire une analyse antivirale et comportementale de l'appareil**
   Réaliser une analyse et une surveillance approfondie de l'appareil à l'aide d'une solution de type EDR (Endpoint Detection and Response).

9. **Réinstaller les systèmes touchés.**
   Effectuer une restauration complète des systèmes infectés. Reformater les postes ou serveurs touchés, effectuer ou faire effectuer une réinstallation complète de ces équipements puis restaurer les données depuis une sauvegarde réputée saine.

10. **Reconnecter le ou les matériels**
    A cette étape, il est crucial d'avoir une estimation raisonnable de la non-persistance des attaquants. Une reconnexion trop tôt du système d'information à Internet peut permettre aux attaquants de continuer leurs actions malveillantes. Aussi, la connexion au réseau ou à internet du ou des matériels ne peut être effectuée que si la source de l'infection a été identifiée et corrigée.

11. **Effectuer un retour d'expérience**
    Le retour à un fonctionnement normal peut être attendu plusieurs semaines voire plusieurs mois après la survenance de l'attaque. Il peut être intéressant de faire un retour d'expérience pendant cette période de convalescence afin de déterminer les pistes d'amélioration mais aussi les points encore sensibles ou problématiques.

PRÉFET
DE LA LOIRE-ATLANTIQUE
Liberté
Égalité
Fraternité

Les mesures préventives

1. Sauvegarder les données
   Des sauvegardes régulières de l'ensemble des données, y compris celles présentes sur les serveurs de fichiers, d'infrastructure et d'applications métier critiques doivent être réalisées. Il s'agit de garder à l'esprit que ces sauvegardes peuvent aussi être affectées par un rançongiciel.
   La règle de sauvegarde 3-2-1 est une méthode recommandée pour ce cas de figure. Elle consiste à avoir **3** copies dess données (l'original + 2 copies de sauvegardes), sur **2** supports de stockages différents (par exemple 1 copie sur disque dur externe et 1 copie sur système de bande) et enfin 1 copie hors site et hors connexion (pour éviter que l'attaquant ne détruise ce jeu de données).

2. Maintenir à jour les logiciels et les systèmes
   Les vulnérabilités non corrigées des systèmes d'exploitation ou des logiciels présents sur le système d'information peuvent être utilisées pour infecter le système ou favoriser la propagation de l'infection.

3. Sensibiliser les collaborateurs
   Le plus souvent, l'attaque par rançongiciel commence par l'ouverture d'une pièce jointe piégée ou la consultation d'une page web malveillante. Ainsi la formation des utilisateurs aux bonnes pratiques de sécurité numérique est une étape fondamentale pour lutter contre cette menace même si elle ne constitue pas un rempart absolu.

4. Mettre en œuvre un plan de réponse au cyber attaque
   La spécificité des attaques par rançongiciel est leur potentiel effet déstabilisateur sur les organisations. Les fonctions support comme la téléphonie, la messagerie mais aussi les applications métier peuvent être mises hors d'usage. Il s'agit alors de passer en fonctionnement dégradé et dans certains cas, cela signifie revenir au papier et au crayon. L'attaque cause en général une interruption d'activité partielle et, dans les cas les plus graves, une interruption totale. Il est donc crucial pour les organisations de définir un plan de réponse aux cyberattaques associé au dispositif de gestion de crise – quand il existe – visant à assurer la continuité d'activité puis son retour à un état nominal.

D'autres mesures : https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes

Les contacts indispensables

- Votre prestataire informatique de réponse à incident
- Pays de la Loire Cyber Assistance (24/7) 0 800 100 200 (Région Pays de la Loire) https://www.paysdelaloire.fr/economie-et-innovation/entreprise/mon-organisation-subit-une-cyberattaque
- e-Collectivités (OPSN) : https://ecollectivites.fr/
- Cybermalveillance.gouv.fr (GIP): Assistance aux victimes de cybermalveillance
- Centre d'assistance de l'ANSSI (CERT-FR) : https://cyber.gouv.fr/en-cas-dincident
- Police/Gendarmerie

PRÉFET
DE LA LOIRE-
ATLANTIQUE
Liberté
Égalité
Fraternité

Les ressources

- Attaques par rançongiciel, comment les anticiper et réagir en cas d'incident : https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes
- Fiche réflexe Rançongiciel : https://www.cybermalveillance.gouv.fr/medias/2019/11/230417_FicheReflexe_Rancongiciels.pdf
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique : https://cyber.gouv.fr/publications/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique
- Anticiper et gérer sa communication de crise cyber : https://cyber.gouv.fr/publications/anticiper-et-gerer-sa-communication-de-crise-cyber
- Fiche sur « les mises à jour » de Cybermalveillance : https://www.cybermalveillance.gouv.fr/medias/2020/04/fiche_mises_a_jour.pdf
- Fiche sur « les sauvegardes » de Cybermalveillance : https://www.cybermalveillance.gouv.fr/medias/2020/04/fiche_sauvegardes.pdf
- Fiche sur « les rançongiciels » de Cybermalveillance : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares
- Guide AMF/ANSSI « Cybersécurité : toutes les communes et intercommunalités sont concernées » : https://medias.amf.asso.fr/docs/DOCUMENTS/7c2acc76b74e58eb04d852c5eb1889ca.pdf

PRÉFET
DE LA LOIRE-
ATLANTIQUE
Liberté
Égalité
Fraternité

Annexe 1 Fiche réflexe à destination des agents

FICHE REFLEXE
INCIDENT CYBER

Les consignes suivantes doivent être appliquées

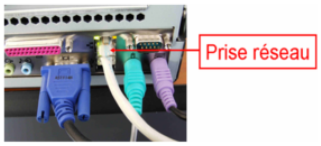
immédiatement après le déclenchement de l'antivirus ou en cas de fonctionnement anormal de l'ordinateur.

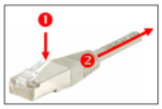
1. DÉCONNECTER LA MACHINE DU RESEAU
2. NE PAS ÉTEINDRE L'ORDINATEUR
3. **RENDRE COMPTE IMMÉDIATEMENT A VOTRE RESPONSABLE INFORMATIQUE**
4. IDENTIFIER CLAIREMENT LA MACHINE COMME INFECTÉE **PAR L'APPOSITION D'UN VISUEL (étiquette,post-it etc..).**
5. INTERDIRE L'ACCÈS A CETTE MACHINE.
6. RASSEMBLER TOUS LES SUPPORTS INFORMATIQUES (Clés USB, disque externe, etc...) UTILISÉS SUR L'ORDINATEUR ET LES CONSERVER.

☎ Prévenir le service informatique / Responsable informatique

Déconnexion du réseau :

Identifier la prise réseau (exemple ci-contre) allant de l'ordinateur à la prise murale et la déconnecter de l'ordinateur en appuyant sur la petite languette située sur la prise.





Source : ©Alpi (https://www.alpi40.fr)