RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

Direction départementale
des Finances publiques du Pas-de-Calais
Mission Départementale Risques Audit
5, rue du Docteur Brassart - BP30015
62034 Arras cedex
Téléphone : 03 21 23 68 00

Mél : ddfip62.mdra@dgfip.finances.gouv.fr

Fiche de vigilance sur les rançongiciels

Un **rançongiciel** (« ransomware » en anglais) est un logiciel malveillant qui bloque l'accès à un ordinateur ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

Le poste informatique peut être infecté suite à une intrusion dans le système, après avoir ouvert une pièce jointe ou cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis dont un cybercriminel a pris le contrôle.

Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes qui peuvent ainsi perdre définitivement toutes leurs données et leurs historiques sur plusieurs années.

Le but de ces attaques est généralement d'extorquer des sommes d'argent (y compris par crypto-monnaies de type « bitcoin ») contre le déblocage supposé du système d'information et l'accès aux données chiffrées. Dans certains cas, le but est uniquement d'endommager le système d'information de la victime pour lui faire subir des pertes d'exploitation et porter atteinte à son image.

Actions à mettre en oeuvre par la collectivité ou l'établissement public victime :

Il est recommandé à la collectivité ou l'établissement public de :

- débrancher le poste de travail infecté ;
- éteindre les serveurs et couper leur accès internet ;
- ne pas connecter les serveurs de sauvegarde aux ordinateurs, ni même aucun autre équipement périphérique (clé USB, ...) ;
- alerter immédiatement les services informatiques de la collectivité ou de l'établissement, ainsi que l'éditeur du logiciel de gestion financière ;
- ne pas payer la rançon réclamée (le paiement ne garantit pas un déblocage total et définitif du système d'information et pourrait inciter le cybercriminel à réitérer son action) ;
- avertir la Préfecture ou l'ARS de ce dossier ;
- déposer plainte auprès des services de police ou de gendarmerie ;
- identifier, si possible, la source et le périmètre de l'infection et prendre les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

La collectivité ou l'établissement pourra appliquer une méthode de désinfection lorsqu'elle existe. En cas de doute, il convient d'effectuer une restauration complète de l'ordinateur infecté : reformatage du poste, réinstallation d'un système sain puis restauration des copies de sauvegarde des fichiers perdus lorsqu'elles sont disponibles, et seulement après avoir obtenu l'assurance que ces copies de sauvegarde ne sont pas elles-mêmes porteuses du rançongiciel.

Il est conseillé aux victimes de se tourner vers un prestataire spécialisé dans la cybermalveillance, et non pas uniquement leur mainteneur habituel.

Un site gouvernemental est dédié à ce type d'escroqueries, et peut permettre à la collectivité de trouver un prestataire : https://www.cybermalveillance.gouv.fr.

Les collectivités territoriales sont par ailleurs tenues de déclarer leurs incidents aux autorités (CNIL, ANSSI, etc.), notamment lorsque ces derniers ont un impact élevé.

Mesures préventives :

- Utiliser des mots de passe suffisamment complexes et les changer régulièrement ;
- Appliquer de manière régulière et systématique les mises à jour de sécurité du système
et des applications/programmes installés sur les postes informatiques ;
- Tenir à jour l'antivirus et configurer le pare-feu ;
- Faire des sauvegardes régulières des données pour pouvoir les réinstaller dans leur état d'origine au besoin et stocker ces sauvegardes sur un équipement totalement déconnecté du réseau informatique ;
- Désinstaller les applications ou programmes dont l'éditeur n'assure plus de support (absence de mise à jour de sécurité) ;
- N'utiliser un poste de travail en session "administrateur" que très ponctuellement et uniquement pour des opérations d'administration du poste ;
- Ne pas ouvrir les courriels provenant d'expéditeurs inconnus ou d'un expéditeur connu mais dont la structure, la syntaxe, l'orthographe et/ou la teneur du message sont inhabituelles ou vides. Ne pas ouvrir les pièces jointes et ne pas cliquer sur les liens provenant de ces messages ;
- Ne pas installer d'applications ou de programmes « piratés », dont l'origine ou la réputation sont douteuses ;
- Eviter les sites non sûrs ou illicites.

Avant même la survenance d'une attaque, il convient de sensibiliser les ordonnateurs à la nécessité d'assurer une sauvegarde de leurs données via leurs éditeurs ou, en l'absence d'éditeur, d'opter pour un hébergement "solution Cloud" payant qui offre une garantie de sauvegarde ("backup").

Documentation :

- Site gouvernemental https://www.cybermalveillance.gouv.fr/
- Fiche « Les rançongiciels »
- Site internet du SHFDS (Service du Haut Fonctionnaire de Défense et de Sécurité des ministères économiques et financiers) : https://ssi.economie.gouv.fr/motdepasse