

Que faire lorsqu'un de vos dossiers ou fichier a été infecté par le virus locky ?

Guilhem VERGON - 2024-08-02 - Issues and solutions

Si votre dossier est synchronisé par NetSync, il convient de mettre en pause l'outil, pour ne pas que le poste infecté ait le temps de synchroniser les documents cryptés.

Une fois les fichiers infectés et cryptés sur la plateforme, vous avez **2 solutions** :

- **Faire appel à notre service support** pour qu'un technicien restaure les données à une date antérieure à l'infection.
- **Récupérer manuellement vos fichiers** depuis les corbeilles des utilisateurs.

Pour en savoir plus sur ce virus locky, c'est par [là!](#)

Faire appel à notre service support

Si vous souhaitez que notre équipe intervienne et s'occupe de tout, nous pouvons mobiliser un technicien sur une demie journée pour qu'il restaure les données: c'est donc une prestation facturable.

Vous pouvez vous adresser directement à notre service commercial au **05 61 61 20 10** qui déclenchera la procédure.

Récupérer manuellement vos fichiers

Pour chaque document infecté, il vous faut:

- **Rechercher l'auteur de la dernière modification** du fichier (ou le dernier ajout) via les **ÉVÈNEMENTS**,
- **Restaurer le fichier** depuis **sa** corbeille utilisateur,
- Une fois restauré, il faut **supprimer la dernière version du fichier**. Pour savoir comment supprimer une version d'un fichier, c'est par [là!](#)

Exemple: votre fichier Schéma support NetExplorer.docx fait parti des fichiers cryptés et vous voulez le récupérer.

1. Les journaux d'évènements

- Dans les **Evènements**, dans le champs **Mot clé** saisissez: Schéma support et cliquez sur **Filtrer**.

- Repérez l'auteur de la dernière modification (UPDATE) ou le dernier ajout (INSERT). Ici l'utilisatrice Nicomng est l'auteur du dernier INSERT.

2. La corbeille de l'utilisateur

- Rendez-vous dans la corbeille de l'utilisateur Nicomng, repérez le fichier Schéma support NetExplorer.docx

- Sélectionnez le fichier et faites un clic-droit **Restaurer**.

Le document se restaure à son emplacement initial.

- Une fois le fichier restauré, il faut supprimer la dernière version du fichier qui est cryptée.

3. Les détails du fichier

- Dans son emplacement initial vous allez retrouver votre fichier.

- Faites un clic-droit **Détails** pour faire afficher les détails du fichier. Les versions du fichier s'affichent les unes après les autres dans l'onglet ACTIVITE.

Repérez la dernière version, ici la 2, et cliquez sur tout à droite et sélectionnez **Supprimer**.

Confirmez votre action.

La version cryptée est supprimée et vous allez retrouver votre fichier.

Remarques

- En fonction des dégâts causés, il sera préconisé de formater le poste afin de le nettoyer correctement.
- Votre NetSync n'arrive pas à se connecter? Suivez la procédure suivante : [Le compte d'un utilisateur se désactive et son NetSync ne se connecte pas \(identifiant ou mot de passe invalide\)](#)
- En savoir plus sur les ransomwares, c'est par [là!](#)