



Rançongiciels – que faire?

Lors d'un incident en lien avec un rançongiciel, il faut prêter attention aux points ci-après:

Limitation des dommages

Déconnectez immédiatement les systèmes infectés du réseau. À cet effet, retirez le câble réseau de l'ordinateur et déconnectez les éventuels adaptateurs réseau sans fil.

Identification des systèmes infectés

Les fichiers journaux (*logs*), à l'aide desquels il est par exemple possible de repérer des accès aux lecteurs réseau, peuvent aider à identifier les systèmes concernés. Les métadonnées des données cryptées peuvent aussi fournir des indications sur les systèmes infectés, par exemple sur les comptes utilisateurs qui ont produit les données. Pensez aussi à sauvegarder les fichiers journaux.

Détection

Les journaux des serveurs de messagerie électronique, des serveurs proxy et des pare-feux ainsi que d'éventuels logiciels de sécurité permettent de déterminer l'ampleur de l'infection et de détecter les adresses URL et IP des assaillants. Bloquez ces adresses URL et IP sur le serveur proxy interne ou sur le pare-feu. Vous éviterez ainsi une connexion avec l'infrastructure de l'assaillant. En cas d'infection par courriel, certains liens (adresses URL et IP) peuvent parfois être lus assez facilement soit directement dans le courriel (hyperlien) soit dans une annexe.

Dénonciation pénale

L'OFCS recommande de procéder à une dénonciation pénale dans tous les cas. Demandez-vous suffisamment tôt si vous voulez le faire. C'est la police cantonale de votre siège qui est compétente. Vous pouvez trouver le poste de police compétent pour celui-ci sur le site Internet [«Suisse e-Police»](https://www.suisse-epolice.ch/#/search-station)

(<https://www.suisse-epolice.ch/#/search-station>)
(1).

La police vous conseillera pour la suite des opérations, en particulier au sujet de la communication avec les auteurs de l'attaque et du comportement à leur égard. Discutez de l'opportunité d'une intervention immédiate de la police en soutien.

Analyses forensiques

Décidez suffisamment tôt si vous allez effectuer ou non une analyse forensique. Cette analyse est importante surtout si vous entendez déposer une dénonciation pénale. Dans un tel cas, informez déjà dans une phase précoce les autorités de poursuite pénale et discutez des prochaines étapes (observation du maliciel, contre-mesures, etc.).

Il serait judicieux qu'un collaborateur ou un prestataire spécialisés sauvegardent les mémoires tampon et les disques durs avant toute tentative de réparation ou tout redémarrage des systèmes concernés, qui rendent presque impossibles les analyses forensiques consécutives. Si les connaissances spécialisées nécessaires ne sont pas disponibles dans votre autorité, il faudrait faire appel à un expert.

Sauvegarde des données cryptées

Si les copies de sauvegarde ont également été cryptées, il est recommandé de conserver et de sauvegarder ces données cryptées afin qu'il soit possible de les décrypter ultérieurement si une solution pouvait être trouvée. Dans certains cas, les autorités de sécurité et de poursuite pénale ont pu, au cours de leurs investigations, accéder à des clés ou trouver des méthodes de décryptage.

Réinstallation des systèmes concernés

Il est nécessaire de réinstaller les systèmes infectés avant de commencer la restauration des données. Le système d'exploitation utilisé devrait provenir d'un support de données fiable.

À certaines conditions, il est possible de restaurer les données, complètement ou en partie, même en l'absence de copies de sauvegarde. Un décryptage est parfois possible si:

- le rançongiciel n'a pas crypté ou effacé des clichés instantanés (*shadow copies*) dans Windows;
- il existe des instantanés des machines virtuelles ou des versions antérieures des fichiers dans les services en nuage;
- la restauration forensique des fichiers effacés est possible;
- la fonction de cryptage du rançongiciel présente des erreurs ou la clé de décryptage est connue.

Le site <https://www.nomoreransom.org>

(<https://www.nomoreransom.org/fr/index.html>)

⁽²⁾ fournit des conseils pour l'identification des maliciels et vous offre la possibilité de télécharger des clés déjà connues. Nomoreransom.org est un projet commun de la police néerlandaise et d'Europol, auquel la Confédération suisse participe également.

Informations sur le paiement des rançons

- L'OFCS déconseille de payer une rançon. Il n'y a aucune garantie que les criminels ne publieront pas les données ou n'en tireront pas un autre profit après le paiement de la rançon. En outre, tout chantage qui réussit incite les assaillants à continuer, finance le développement des attaques et favorise leur propagation.
- Si vous envisagez quand même de payer une rançon, l'OFCS vous recommande instamment de discuter de ces opérations avec la police cantonale.

Dernière modification 01.01.2024

<https://www.ncsc.admin.ch/content/ncsc/fr/home/infos-fuer/infos-behoerden/vorfall-was-nun/ransomware.html>

Page Links

1. <https://www.suisse-epolice.ch/#/search-station>
2. <https://www.nomoreransom.org/fr/index.html>