La lettre d'Information de LoGeAs

Août 2017

Les Ransomware

Table des matières

Edito

Depuis quelques temps la pratique se répand !

Vous avez probablement dû entendre le terme de ransomware. Cette pratique est très problématique car les solutions pour décrypter les fichiers sont encore rares. Les ransomware évoluant très rapidement, il est difficile de trouver le bon "décrypteur" pour vos fichiers.

Si aucune sauvegarde n'a été faite sur les fichiers impactés,
ils peuvent être perdus à tout jamais.

De plus, ces ransomware sont très difficiles à détecter par les antivirus du fait de leurs évolutions constantes. Rien ne garantit que la solution antivirus que vous possédez les bloqueront, puisque ce n'est pas leur fonction première.

La seule solution valable est la sauvegarde des fichiers, et la restauration en cas d'infection.

Si vous ne disposez pas encore de solution de sauvegarde,
contacter nous, nous saurons vous conseiller !

Vous avez dit « Ransomware » !?

Qu'est-ce qu'un « Ransomware » ?

Le ransomware est un malware, appelé parfois à tort "virus", (ou à raison s'il se duplique et propage de lui-même) qui a pour but final de soutirer de l'argent à sa victime.

L'infection passe par le **téléchargement d'un logiciel malveillant** parfois dissimulé dans la pièce jointe d'un courriel piégé ou au bout d'un lien.

Il peut aussi se diffuser par le biais de **pages web piratées** qui tentent d'utiliser les failles des systèmes d'ordinateurs.

Attention ! Le logiciel tente souvent de se faire passer pour une autorité : police, gendarmerie, FBI, lutte contre le téléchargement illégal etc.

Lorsque le ransomware a pris place sur l'ordinateur de sa victime, il applique un blocage du système ou un chiffrement (**cryptage**) sur les fichiers et dossiers personnels de l'ordinateur, de telle sorte qu'ils deviennent illisibles. Une fois son travail terminé, il indique à l'utilisateur piégé un moyen de débloquer l'ordinateur et de récupérer ses fichiers, généralement en **payant une rançon** contre la clé de cryptage qui permettra d'ôter le chiffrement.

Ne payez jamais cette rançon !
Vous n'avez aucune garantie que le « pirate » vous donnera le moyen de récupérer vos données. Au contraire, il pourrait s'attaquer aussi à vos coordonnées bancaires.

Une fois un fichier chiffré (crypté), il est **impossible de le récupérer,** à part si une société parvient à trouver une méthode de décryptage et fournit gracieusement sa solution.

Comment se protéger ?

Redoubler de prudence avec vos e-mails

Les e-mails sont la **première source d'infection**. Pour s'en protéger, il existe différentes attitudes à adopter :

- **Vérifier l'expéditeur du mail si celui-ci contient une pièce jointe**

Les courriels frauduleux sont souvent envoyés d'une adresse pouvant facilement être confondue avec une adresse valide. Ce qui est important dans une adresse e-mail se trouve après le "@" et non avant.

Par exemple Google ou encore Facebook ont des adresse se terminant par @google ou @facebook. Donc si vous recevez un courriel provenant de facebook@security, vous devez en déduire que l'adresse n'est pas authentique et qu'elle représente sûrement une tentative de phishing ou autre. Vous devez donc redoubler de précaution !!!

- **Ne jamais ouvrir une pièce jointe si l'expéditeur n'est pas confirmé !**

Sur vos PC personnels vous faites ce que vous voulez, mais pas au travail ;)
Pour plus de sécurité, bloquez le contenu distant des courriels dans votre logiciel de messagerie, activer-les uniquement au cas par cas.

Attention sur internet :

- **Il faut être sûr du site sur lequel vous téléchargez vos fichiers.**

Ne pas télécharger n'importe quoi sous prétexte qu'un collègue ou un site vous le conseille.

Les sites très connus du type 01net.com ou clubic, proposent un grand nombre de logiciels à télécharger et sont très pratiques, mais ils ajoutent souvent dans leurs installateurs des adware et autres PUP (Potentially Unwanted Program). Ces programmes ajoutent des barres de recherche dans vos navigateurs, changent vos pages par défaut des navigateurs internet etc.

- **Il est recommandé de toujours télécharger le logiciel sur le site de l'éditeur original.**

par exemple pour télécharger Google Chrome, il faut se rendre sur le site de Google et non sur 01net et consorts.

- **Prudence avec les sites de streaming (et autres sites « illégaux »).**

Évitez de cliquer sur les boutons du type "Regarder le dernier Avenger gratuitement en full HD". Il est rarement aussi facile de trouver un fichier dit "pirate". Si vous avez un navigateur Google Chrome ou Firefox et que vous tenez tout de même à télécharger ce genre de fichier, pensez à installer un bloqueur de Pub de type « uBlock Origin ». Cet Ad On limitera le nombre le liens et pubs vous renvoyant vers des virus et autres logiciels malveillants.

- **Lire attentivement les messages.**

Il ne faut pas cliquer sur "OK" ou "Suivant" tout le temps ! prenez le temps de lire et de comprendre ce que le logiciel essaye de vous dire avant de continuer.

Une seule protection : la sauvegarde …

Qu'ai-je d'important dans mon ordinateur ?

Quand on commence à réfléchir à la protection contre la perte des données de son ordinateur, cette question est primordiale, et une réponse aussi détaillée que possible est importante. Trop souvent nous rencontrons dans notre clientèle des utilisateurs qui n'ont aucune idée des informations stockées et encore moins de leur emplacement.

Voici quelques pistes à suivre :

- Vous utilisez votre poste pour y faire du courrier, des tableaux … (*Nous vous conseillons de toujours les regrouper dans un seul et même répertoire, que vous subdiviserez en sous- répertoires par thème. Cela facilitera la sauvegarde. Sous Windows, utilisez par exemple*, « *Mes Documents* ».)
- Vous utilisez un logiciel de messagerie (Outlook, Thunderbird …) les messages sont peut-être très importants (facture, code, courrier important …)
- Vous utilisez Internet, et stockez souvent sans vous en rendre compte des adresses de sites, des mot de passe ...
- Vous utilisez votre ordinateur pour stocker vos photos (souvent vous ne les tirez plus sur papier), vos vidéos
- Vous utilisez des logiciels tiers qui stockent des informations dans des dossiers spécifiques, comme par exemple LoGeAs, qui enregistre le fichier de l'association et sa comptabilité

Différence entre « archivage » et « sauvegarde »

L'archivage a pour but de permettre la consultation à moyen ou long terme des documents qui peuvent être importants (comptabilité...) voire patrimoniaux (archives …). Préférez toujours le papier. Les formats des fichiers évoluant rapidement, il est possible que le document, sur informatique, soit inutilisable au bout de quelques années.

La sauvegarde a pour but, elle, de permettre la reprise des documents en cours de vie pour éventuellement les faire évoluer ou pour effectuer des analyses … Pensez à relire régulièrement vos supports en les faisant évoluer afin d'éviter tout problème d'obsolescence du format du fichier. Parmi les formats qui semblent un peu plus pérennes que d'autres, on peut envisager le format PDF pour les textes et le format JPG pour les images.

Quels risques courent mes données ?

Vos données sont généralement stockées dans votre ordinateur sur un disque dur ou un SSD (sorte de grosse clef USB). Le risque principal est donc un disque qui ne fonctionne plus.

Une fois ce problème anticipé, deux autres risques guettent votre ordinateur :

- le vol : aussi une règle s'impose : ne JAMAIS stocker ses sauvegarde avec son ordinateur ;
- un logiciel malveillant (virus, ransomware, ...)

Et enfin le dernier risque, et malheureusement pas le moindre, c'est vous …. Il est très facile de perdre des données dans une fausse manœuvre.

Quelles sont les bases d'une bonne sauvegarde ?

Le multisupports :

La sauvegarde n'est pas faite uniquement sur un seul support, mais sur plusieurs, afin de se prévaloir contre la défaillance de l'un d'eux.

Le multi-sites :

la sauvegarde doit être déposée dans plusieurs sites physiques pour éviter les problèmes locaux.

Le multi-systèmes d'exploitation :

la plupart des virus informatiques sont spécifiques à un système d'exploitation (par exemple un virus Windows sera inopérant sur un serveur Linux). Si la sauvegarde est faite sur un système différent de celui sur lequel vous travaillez, vous augmentez vos chances en cas de propagation d'un virus destructeur.

La maintenance d'un historique :

imaginons que le système de sauvegarde mis en place consiste à sauvegarder tous les soirs le fichier clients de votre entreprise sur un support unique que vous emportez chez vous. Si votre base se corrompt sans que vous vous en aperceviez et que vous écrasez votre fichier par mégarde, à partir de quoi restaurerez-vous vos sauvegardes ? Il faut absolument disposer de plusieurs jeux de sauvegarde (celle de la veille, de la semaine passée…) il vaut toujours mieux revenir à l'état du fichier de la semaine passée que tout perdre !

La simplicité du système :

s'il vous faut une heure de manipulation pour réaliser votre sauvegarde, combien de temps le ferez-vous sérieusement ?

Le coût :

permettre une restauration possible à coût faible et un coût d'exploitation raisonnable

Le lieu de stockage :

le disque, la clef … NE DOIT PAS ÊTRE CONNECTE en permanence à votre ordinateur, notamment au regard des ransomware qui encrypte tous les disques accessibles depuis le système.

Quels moyens à mettre en place ?

Il existe plusieurs voies pour sauvegarder vos données :

Tout sauvegarder :

Il existe des logiciels qui proposent de sauvegarder l'ensemble de votre poste (on parle d'image du disque). Même si cette solution semble intéressante, elle n'est pas conseillée en terme de sauvegarde de données, car elle est longue et difficile à mettre en œuvre.

Copier mes données sur un disque :

Le support externe peut être un disque dur, une clef USB … Il est alors possible de faire :

- une copie manuelle fichier par fichier ou une copie des répertoires importants (Attention de ne pas en oublier !)
- une copie assistée par un logiciel, qui peut avoir le grand avantage de ne recopier que les documents modifiés depuis la sauvegarde précédente. Attention alors de toujours sauvegarder les nouveaux fichiers dans les répertoires sauvegardés. Il est même possible de programmer le logiciel pour qu'il réalise la sauvegarde régulièrement et automatiquement.
- Une autre piste à explorer dans le cas où vos données sont importantes : c'est la solution NAS. Il s'agit de petits ordinateurs (à partir de 150€) dédiés au stockage. Ils proposent des solutions qui permettent, par la redondance de disques durs, de palier à la casse de l'un d'eux. Évitez toujours de les mettre trop prêt du poste principal à cause du vol.

Envoyer mes données par courriel :

Certains fichiers ou sauvegardes sont suffisamment « petits » pour être envoyés en pièce jointe à une autre personne qui a pour mission de les garder au cas où. C'est par exemple le cas des sauvegardes de LoGeAs à l'archivage.

Envoyer mes données sur une sauvegarde en ligne (CLOUD):

Si vous ne souhaitez pas investir dans du matériel pour sauvegarder vos fichiers, ou parce que ceux-ci ne pèsent finalement pas lourd, vous pouvez vous tourner vers une solution en ligne. Il y en a pléthore et la plupart, gratuites ou aussi payantes, vous offrent plusieurs Go d'espace de stockage. Sachez tout de même que vous données seront conservées sur des serveurs qui eux-mêmes peuvent être endommagés. Deux copies valent donc mieux qu'une !

En guise de conclusion

Vous disposez de tout le contenu imaginable à portée de clic, profitez-en !

La plupart des questions que vous pourrez vous poser ont probablement déjà été abordées et solutionnées sur différents forums et sites internet. Tout ce qui vous reste à faire est de trouver la bonne formulation pour exposer votre problème sur internet et consulter le contenu en conséquence.

Si vous avez un doute, n'hésitez pas à nous contacter. Nous saurons vous conseiller quant à l'action à entreprendre.

N'oubliez pas qu'il est toujours plus facile d'agir en amont que de corriger quand il est trop tard !

Merci à tous pour votre attention et votre vigilance future.

courriel : assistance@logeas.fr
Téléphone : 05 61 88 91 68
22 rue Saint Genest
31800 Labarthe Inard

Sauvegarde de vos bases
(et uniquement ça)
Sauvegarde@logeas.fr

Comptabilité, programmation de formation, …
Émail : contact@logeas.fr
Téléphone : 05 61 88 91 68 Télécopie 09 72 13 22 08
22 rue Saint-Genest – 31800 Labarthe-Inard