Ransomware ou crypto-ransomware

Guilhem VERGON - 2022-03-23 - Problèmes et solutions

Ransomware ou crypto-ransomware

Vous avez ouvert un **mail avec une pièce jointe malveillante** ou bien **téléchargé un programme sur Internet** et vous vous retrouvez avec des noms de fichiers que vous n'aviez pas auparavant comme ci-dessous:

akX0R4PUmv.zepto	08/11/2016 10:15	Fichier ZEPTO
bdhusoznlp.odin	08/11/2016 10:16	Fichier ODIN
joihbbkhuo.ttt	08/11/2016 10:16	Fichier TTT
ojbzsVZFm.aeab	08/11/2016 10:15	Fichier AEAB

Quand vous tentez d'ouvrir ces fichiers, vous accédez à un contenu qui n'est pas le vôtre.

Vos données ont été chiffrées et dans un fichier texte souvent appelé Readme stocké sur votre bureau, on vous **demande de payer une somme d'argent** pour récupérer vos données à l'aide d'une clé de déchiffrement.

→ Vous avez été attaqué par un ransomware.

Qu'est-ce qu'un ransomware?

Très courant ces derniers mois, les ransomwares, ou rançongiciel en français, sont des

logiciels malveillants qui chiffrent vos données pour les rendre inutilisables ou bien **bloquent votre ordinateur** et vous demande de payer une rançon pour y accéder de nouveau.

Ransomware

On distingue:

- **les ransomwares à chiffrement :** qui chiffrent vos données pour les rendre inutilisables sans la clé de déchiffrement.
- **les verrouilleurs :** qui bloquent votre poste.

La plupart des ransomwares utilisent un algorithme de chiffrement solide qui est très difficile à outrepasser. Il faut donc obligatoirement une clé de déchiffrement pour récupérer vos données.
Il est formellement déconseillé de payer la rançon demandée. Vous n'avez en effet aucune garantie que vos données soient de nouveau utilisables après le paiement et en finançant cette rançon vous alimentez le développement de ce type d'attaques. Ces dernières ont été estimé à 24 millions de dollars en 2015.

Comment l'infection se déroule-t-elle?

Le plus souvent l'infection se propage toute seule à l'ouverture d'une pièce jointe malveillante glissée sur un mail. L'exécution du ransomware est donc totalement transparente pour l'utilisateur.
En général, le ransomware apparait clairement à l'écran pour l'utilisateur dès qu'il a fini de chiffrer vos données. Mais à ce moment là, il est déjà trop tard pour les sauver.
Ainsi, il peut se passer plusieurs jours entre le moment où vous êtes infecté et celui où le virus se matérialise souvent via un fichier .txt ou Readme.

Types de fichiers qui peuvent contenir un ransomware:

- les exécutables (.exe ou .scr)
- les dossiers compressés en .zip ou .rar
- les fichiers Office (.doc, .doxw, xls, xlsx, ppt, pptx,...) avec des macros vulnérables
- les raccourcis.

Si vous n'avez pas de sauvegarde de vos données sur votre poste, il est probable que vos fichiers chiffrés soient irrécupérables.
En revanche si vous les avez synchronisées avec NetExplorer, vous allez pouvoir les récupérer.

Procédure à suivre

Voici la procédure à suivre lorsque vous avez été infecté:

1 - Vérifier les **derniers ajouts de fichiers** depuis les journaux d'évènements de la plateforme et **repérer les extensions malveillantes**.
2 - Faire une **recherche avec la ou les extensions malveillantes sur la plateforme** et **supprimer les résultats**.
3 - **Restaurer** depuis votre corbeille utilisateur sur la plateforme les éléments qui ont été déplacés suite au chiffrement.
4 - Sur les dossiers restaurés, remettez les droits d'accès directement depuis la plateforme.
5 - Sur le poste infecté, faites une **recherche sur vos disques** avec la ou les extensions malveillantes et **supprimer les résultats**.
6 - Faites un **scan anti-virus** sur votre poste pour s'assurer qu'il n'est plus infecté.

Les données stockées sur votre plateforme sont récupérables directement depuis vos corbeilles utilisateurs.
En revanche, sur votre poste, si vous avez des données qui ne sont pas synchronisées avec notre solution, alors il se peut que vous les ayez perdues suite au chiffrement.

Si vous le souhaitez, nous pouvons vous proposer une solution de nettoyage clé en main. Pour cela vous pouvez contacter directement notre service commercial au **05 61 61 20 10**.

Quelques recommandations

- **Avoir un anti-virus installé et à jour** sur votre poste.
- Faites également régulièrement les **mises à jour de votre système d'exploitation.**
- **Être vigilant lorsque vous ouvrez des pièces jointes** depuis un mail. Ouvrez-les uniquement si vous connaissez l'expéditeur.
- Ne pas cliquer sur tous les liens que l'on vous envoie.
- **Privilégier des solutions de stockage en ligne comme NetExplorer** au lieu de conserver vos éléments sur vos postes localement.

Attention: Même en ayant un MAC, vous pouvez être infecté par un ransomware. Il en est de même sous Linux.

Filtrage des extensions malveillantes

Enfin, sachez que nos outils filtrent les extensions malveillantes pour éviter de contaminer vos données synchronisées avec NetExplorer. Voici la liste des extensions filtrées:

Extensions considérées comme dangereuses			
1999	_crypt	0x0	aaa
abc	aeab	bleep	ccc
crinf	crjoker	crypt	crypto
CTB2	CTBL	ecc	ekybtc
@inbox_com	EnCiPhErEd	encrypted	encryptedRSA
exx	ezz	good	HA3
LeChiffre	locked	locky	LOL!
magic	micro	odin	OMG!
pzdc	R16M01D05	r5a	RDM
ROGER	RRK	SUPERCRYPT	XTBL
toxcrypt	ttt	vault	vvv
XRNT	xxx	zzz	zepto

Si vous tentez de déposer un fichier avec une extension citée ci-dessus, il ne sera pas uploadé peu importe l'outil que vous utilisez (NetSync, la plateforme,...).
Votre compte utilisateur pourra même se désactiver automatiquement si vous tentez de déposer un fichier malveillant.

En revanche, il est possible que le virus impacte vos données synchronisées, si l'extension n'est pas encore connue.
En effet, chaque semaine, de nouveaux ransomwares sont crées et il est difficile de tous les connaitre.

Nous essayons de mettre à jour régulièrement nos listings mais il se peut, en cas de nouvelle extension, qu'elle ne soit pas bloquée automatiquement. Dans ce cas, les fichiers cryptés apparaitront dans votre LIBRAIRIE et vos fichiers seront dans la corbeille de l'utilisateur impacté par le ransomware. Vous pourrez récupérer vos fichiers en les restaurant.

Les ransomwares connus

Il est difficile d'établir un listing exhaustif des ransomwares connus puisque de nouveaux ransomwares apparaissent tous les jours.
Cependant voici les plus connus en France: *Locky, Petya, CryptXXX, TeslaCrypt, Cerber, CTB Locker,*...