INFORMATIQUE

Alerte aux virus-rançon

Rappel des principes de base de la sécurité informatique

Par Fabien CLEUET, Auditeur CISA membre de l'AFAI, Expert de justice, Vice-président de la Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées (www.cnejiat.org), Médiateur Carbileb

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) le confirme, les virus-rançon pullulent, notamment depuis décembre 2015 [1]. Ils sont particulièrement dangereux pour les organisations, quelle que soit leur taille. On les appelle *crypto-locker* (ou *ransomware*), car leur principe consiste à extorquer de l'argent après avoir bloqué l'accès à un système ou à ses données. Souvent basé sur le virus *TelsaCrypt*, il s'agit d'une pièce jointe à un mail (souvent cachée dans un fichier zip) qui appelle puis exécute un programme qui va crypter la majeure partie des fichiers de MS Office (dont Word, Excel, Outlook notamment). Le virus agit silencieusement, sans que l'utilisateur n'en soit nécessairement alerté.

Une fois les données cryptées, Le décryptage est proposé moyennant la fourniture d'un code qui coute 300 à 500 USD. Attention, ce virus ne s'arrête pas au poste qui reçoit le courriel, mais aussi aux disques partagés ou connectés depuis le compte de l'utilisateur. TelsaCrypt ou d'autres ransomware tels CBT-Locker ou Ransom.Win32.Bitman, sont donc de véritables fléaux d'autant qu'ils ne sont généralement pas décelés par les antivirus qui sont censés sécuriser l'utilisateur. Lorsque ce dernier constate le problème, il est déjà trop tard.

Pour résumer, l'activation de ce virus interdit l'accès aux documents bureautiques et à la messagerie Outlook. En conséquence, cela peut perturber lourdement les activités dépendant de ce type de documents. Le prix modéré de la rançon rend l'action judiciaire sans perspective.

Faut-il payer la rançon ?

La question ne se pose pas si l'entité dispose de sauvegardes exhaustives et fiables qui n'ont pas été contaminées. Mais en réalité, de nombreuses organisations constatent rapidement qu'elles n'ont pas d'autre choix que de payer. Pour autant, rien n'assure que les codes fournis vont effectivement restaurer tous les fichiers corrompus. Il ne faut pas attendre d'honnêteté ou de service après-vente de la part d'un maître chanteur.

Faut-il chercher des solutions de décryptage sur le net ?

Ici encore, outre le temps passé, il ne faut pas imaginer trouver une solution rapide et fiable par soi-même, en deux requêtes Google. Seul un informaticien solide ayant déjà réussi une telle opération a une chance raisonnable d'y parvenir.

L'intelligence de ce piratage est la combinaison de sa capacité de nuisance très force, la quasi-impossibilité de s'y soustraire techniquement et le faible coût de la rançon. Dans la plupart des cas, les entreprises ont réussi à restaurer les données ou payé. Aucune n'a porté plainte ou signalé l'intrusion aux agences CERT, ANSSI ou autre. C'est pourquoi les estimations sur la fréquence de ces virus sont sous-évaluées.

Quel bilan de la situation ?

Dire que l'internet n'est pas sécurisé ne constitue pas une nouveauté. On peut faire le même grief aux systèmes d'exploitation de nos ordinateurs, à commencer par Windows même en tenant compte des efforts entrepris. Dans un tel contexte, il faut espérer de réelles améliorations des antivirus externes et internes qui à ce jour, restent aveugles à l'égard de ces risques.

Comment se prémunir du risque ?

La seule solution durable et fiable est la sauvegarde et surtout l'éducation et la sensibilisation des utilisateurs. Il faut agir sur le facteur humain qui reste le maillon faible de la sécurité :

- mettre en place une charte des utilisateurs qui explique les enjeux, les risques, les droits ET les devoirs,
- renouveler régulièrement les consignes, tout particulièrement s'agissant des courriels émis par des inconnus dont les pièces jointes sont a priori suspectes.

En amont, l'approche préventive rappelle les (vieux) principes de la sécurité informatique :

- avoir des sauvegardes régulières, exhaustives, contrôlées et non connectées de manière permanente,
- sensibiliser régulièrement les utilisateurs pour qu'ils adoptent les réflexes de prudence essentiels,
- faire auditer la sécurité du système d'information sous un angle organisationnel et non exclusivement technique.

Lorsque le virus a frappé, la solution curative impose de :

- déconnecter immédiatement du réseau la machine recevant le pourriel (car la propagation se fait via les partages de disques) ;
- consulter les instructions du CERT [2] ;
- réinstaller totalement chaque machine infectée (système d'exploitation et application) ;
- restaurer les sauvegardes de données en espérant qu'elles soient exhaustives, à jour et fiables. Dans le cas contraire, on peut imaginer la désorganisation qui en résulte.

Force est de constater que certaines mesures de sécurité ne varient pas… une bonne sauvegarde reste incontournable, tout autant que les mesures préventives qui permettent de ne pas les utiliser.

Après ce virus, actuellement non décelé par la majorité des logiciels antivirus, d'autres menaces prendront le relai. Il importe donc de maintenir la vigilance des utilisateurs, car le facteur humain est généralement le maillon faible de la sécurité informatique.

Dans le domaine de la sécurité de l'information, l'expert-comptable est un conseil précieux de l'entreprise en commençant par diffuser et expliquer ces informations essentielles. ■

1. http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ALE-015/index.html

2. http://www.cert.ssi.gouv.fr