Le rançongiciel, ransomware ou malware de rançonnage : définition, protection et sanctions juridiques

Fiche pratique publié le **04/05/2022**, vu **1919 fois**, Auteur : Anthony BEM

Qu'est-ce que le ransomware ? Quels sont les moyens de protection contre le ransomware ?

Depuis les années 1980 et la généralisation des ordinateurs dans les foyers, une nouvelle forme de criminalité technologique s'est développée au travers de virus informatiques ingénieux.

Le rançongiciel ou ransomware est un logiciel malveillant consistant en la diffusion d'un virus afin de bloquer l'accès à un ordinateur ou à ses données en les chiffrant.

Le but de ce virus est d'empêcher les utilisateurs d'accéder à leur système ou à leurs fichiers personnels et de leur réclamer le paiement d'une somme à titre de rançon pour pouvoir en obtenir de nouveau l'accès.

Ainsi, un ransomware a pour objectif d'obtenir de l'argent de la victime, souvent en Bitcoin ou en cryptomonnaies, en échange de la clé qui permettra le déchiffrage des données ou la récupération des systèmes.

Aujourd'hui, les entreprises privées, les établissements de santé, les collectivités locales et les professionnels du droit en sont les principales victimes.

Concrètement, l'ordinateur ou le système d'information de la victime peut être infecté :

-après la réception d'un e-mail malveillant contenant une pièce jointe piégée. Les malspams peuvent inciter les utilisateurs à ouvrir les pièces jointes ou à cliquer sur des liens qui semblent provenir de sources légitimes, comme celle d'un ami ou d'une institution,

-en naviguant sur un site internet infecté. Le malvertising, ou publicité malveillante consistant en l'utilisation des publicités en ligne pour distribuer des malwares aux utilisateurs qui peuvent être renvoyés vers des serveurs criminels sans avoir même cliqué sur une seule publicité,

-à la suite d'une intrusion dans le système informatique depuis ses accès ouverts sur l'extérieur (travail à distance, maintenance…),

-après l'installation d'une application ou d'un programme piraté.

En outre, Il existe deux grands types de ransomwares :

-les verrouilleurs d'écran ou lockerwares qui bloquent l'accès à un ordinateur;

-les ransomwares chiffreurs de fichiers ou cryptowares qui cryptent des données sur l'ordinateur.

L'attaquant adresse alors un message à la victime pour lui proposer de lui fournir le moyen de déchiffrer ses données contre le paiement d'une rançon.

Il est intéressant de souligner que les auteurs de malwares ciblent aussi les mobiles ou les Mac en copiant des fichiers malveillants qui s'exécutent silencieusement en arrière-plan malgré l'existence d'anti-malware intégré d'Apple.

La victime d'une attaque de ransomware ne doit jamais céder au chantage et payer la rançon afin de ne pas encourager les cybercriminels à poursuivre leurs attaques contre elle ou contre des tiers. Surtout le paiement de la rançon ne garantit pas que l'ensemble des données soit restituées et n'immunisera pas la victime contre de nouvelles attaques.

Néanmoins, il existe des experts en sécurité informatique qui peuvent utiliser des déchiffreurs adaptés ou procéder à la restauration complète du système.

Sur le plan juridique, le ransomware est constitutif de plusieurs infractions pénales telles que :

-l'extorsion de fonds ;

-l'introduction frauduleuse dans un système de traitement automatisé de données informatiques;

-l'entrave au fonctionnement d'un système de traitement automatisé de données informatiques.

Par conséquent, la victime peut déposer une plainte pénale auprès du procureur de la République du tribunal judiciaire en fournissant toutes les preuves nécessaires.

Il est alors, recommandé d'adresser la plainte pénale au juge, soit avant la réinstallation des ordinateurs, soit de solliciter l'intervention d'un expert informatique qui collectera un maximum de preuves techniques utiles aux enquêteurs. Ces mesures augmenteront les probabilités que la plainte aboutisse à des condamnations des auteurs et à des indemnisations des victimes.

En outre, il peut être encore plus opportun de déposer parallèlement une plainte pénale auprès du juge dans le pays de résidence de l'auteur de l'attaque qui aura pu être identifié dans le cadre de la première procédure.

A cet égard, le recours à un cabinet d'avocats spécialisé en droit international peut s'avérer être opportun.

Les professionnels français doivent aussi adresser à la CNIL une notification en cas d'infection, de modification ou de suppression de données à caractère personnel, et/ou si les données ont été divulguées de manière illicite.

La notification de la violation à la CNIL est nécessaire **dès qu'il y a un risque pour la vie privée des personnes**, que l'incident soit d'origine accidentelle ou illicite.

Cette notification doit intervenir dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, même lorsqu'il s'agit d'une indisponibilité temporaire (articles 33-1 et 55 du RGPD).

Cette notification :

-est une **obligation légale** passible de sanctions en cas de manquement ;

-permet à la CNIL **d'avoir connaissance de l'incident** et, dans les cas les plus graves, **d'orienter** et **de conseiller** les organismes sur la conduite à tenir et les mesures à prendre;

-permet de **déterminer si une communication aux personnes concernées est nécessaire**, dans le cas où elle n'a pas été déjà été réalisée (article 34 du RGPD) afin que ces dernières puissent prendre les mesures appropriées pour limiter les effets de la violation envers elles-mêmes.

Je suis à votre disposition pour toute action ou information (en cliquant ici).

Anthony Bem
Avocat à la Cour
27 bd Malesherbes - 75008 Paris
01 40 26 25 01
abem@cabinetbem.com