Les ransomwares (ou rançongiciels)

Les criminels appliquent toute une série de stratégies pour soutirer de l'argent à leurs victimes inconscientes. Une de leurs méthodes favorites consiste à chiffrer les fichiers de l'utilisateur puis à lui demander une « rançon », en échange de quoi il pourra – peut-être – récupérer ses données.

Voici comment vous protéger contre les rançongiciels :

- **Effectuez régulièrement une sauvegarde de vos données (backup).** Une fois votre sauvegarde effectuée, veillez à bien déconnecter le support de l'ordinateur, sans quoi les données sauvegardées risqueraient elles aussi d'être verrouillées en cas d'infection de l'ordinateur par un rançongiciel.
- **Faites en sorte que les programmes et les plugins installés sur votre ordinateur soient toujours parfaitement à jour.** Assurez-vous de disposer toujours de la dernière version disponible de tous vos logiciels, applications et plugins de navigation. Dans la mesure du possible, recourez systématiquement à la fonction de mise à jour automatique.
- **Faites preuve de prudence lorsque vous recevez des courriels suspects** non sollicités ou provenant d'expéditeurs inconnus. Ne suivez pas les instructions indiquées dans le message, n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens.
- **Utilisez un programme de protection antivirus** et veillez à ce qu'il soit constamment mis à jour par le biais des mises à jour automatiques. Un antivirus non actualisé risque en effet de ne pas reconnaître les derniers logiciels malveillants.

Fonctionnement

Tout va très vite : l'ouverture d'une pièce jointe infectée ou d'un site web piraté suffit parfois pour introduire le rançongiciel dans le système. Une fois inoculé, le programme malveillant efface ou chiffre l'ensemble des fichiers stockés, les rendant de fait inutilisables.

Un écran de verrouillage apparaît sur l'ordinateur, demandant à la victime de payer une rançon au hacker dans une monnaie virtuelle (en bitcoins par exemple), en échange de quoi il procèdera au déverrouillage de ses données. En choisissant une monnaie virtuelle, les cybercriminels savent qu'il sera très difficile de remonter jusqu'à eux.

Or le fait de se plier aux exigences des malfaiteurs et de verser la rançon exigée ne garantit pas que la victime pourra effectivement retrouver l'usage de ses données verrouillées. En agissant ainsi, on finance le modèle opérationnel des cybercriminels qui peuvent ainsi poursuivre leurs attaques et racketter de nouvelles victimes.

Sauvetage possible en cas d'urgence : certains sites web tels que www.nomoreransom.org (https://www.nomoreransom.org/fr/index.html) permettent de voir si des routines de décryptage existent déjà pour tel ou tel ransomware.

Leur cible de prédilection reste les entreprises : dans la mesure où elles disposent de très grandes quantités de données confidentielles et stratégiques, elles sont souvent plus enclines à payer de grosses sommes d'argent pourvu d'éviter la perte de données cruciales. Cela dit, le risque d'infection par un rançongiciel et la perte des données qui en découle touche tout autant les particuliers.

La principale contremesure pour se protéger contre une perte de données provoquée par un rançongiciel est donc de procéder régulièrement à des copies de sauvegarde (backup) – cf. « Règle n°1 – Sauvegarder les données » (https://www.ebas.ch/fr/1-sauvegarder-les-donnees/).

Les rançongiciels (ou ransomware en anglais) font partie de la famille des logiciels malveillants (malwares).

Ceux-ci se diffusent généralement via des pièces jointes ou des sites Internet infectés. Une fois installé, le rançongiciel verrouille les fichiers stockés sur l'ordinateur de la victime ainsi que sur tous les lecteurs réseau et supports de données connectés, comme par exemple les clés USB. À partir de là, la victime ne peut plus accéder à ses données.