Ransomware

Définition

Un rançongiciel (*ransomware* en anglais) est un logiciel malveillant qui bloque l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion sur le système.

Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

But recherché

EXTORQUER DE L'ARGENT à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues.

Certaines attaques visent juste à endommager le système de la victime pour lui faire subir des pertes d'exploitation et porter atteinte à son image.

Mesures Préventives

- Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

- Tenez à jour l'antivirus et configurez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications, services et machines légitimes.

- N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez par sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.

- N'installez pas d'application ou de programme « piratés » ou dont l'origine ou la réputation sont douteuses.

- Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

- Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.

- N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.

- Utilisez des mots de passe suffisamment complexes et changez-les régulièrement, mais vérifiez également que ceux créés par défaut soient effacés s'ils ne sont pas tout de suite changés (notre fiche dédiée aux mots de passe sur www.cybermalveillance.gouv.fr).

- Éteignez votre machine lorsque vous ne vous en servez pas.

Si vous êtes victimes

- DÉBRANCHEZ LA MACHINE D'INTERNET ou du réseau informatique.

- En entreprise, **ALERTEZ IMMÉDIATEMENT VOTRE SERVICE INFORMATIQUE.**

- NE PAYEZ PAS LA RANÇON réclamée car vous n'êtes pas certain de récupérer vos données et vous alimenteriez le système mafieux.

- DÉPOSEZ PLAINTE auprès de la police ou de la gendarmerie ou en écrivant au procureur de la République dont vous dépendez. Faites-vous, au besoin, assister par un avocat spécialisé.

- IDENTIFIEZ LA SOURCE DE L'INFECTION et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

- APPLIQUEZ UNE MÉTHODE DE DÉSINFECTION ET DE DÉCHIFFREMENT, lorsqu'elle existe. En cas de doute, effectuez une restauration complète de votre ordinateur. Reformatez le poste et réinstallez un système sain puis restaurez les copies de sauvegarde des fichiers perdus lorsqu'elles sont disponibles.

- FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS QUALIFIÉS. Vous trouverez sur https://www.cybermalveillance.gouv.fr/ des prestataires spécialisés susceptibles de pouvoir vous apporter leur assistance.

Les infractions encourues

• De tels procédés relèvent de l'extorsion de fonds et non de l'escroquerie. En effet, ils se caractérisent par une contrainte physique – le blocage de l'ordinateur ou de ses fichiers – obligeant à une remise de fonds non volontaire. L'article 312-1 du code pénal dispose que : « l'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. L'extorsion est passible de sept ans d'emprisonnement et de 100 000 euros d'amende ».

• L'infraction d'atteinte à un système de traitement automatisé de données (STAD) pourra aussi être retenue (article 323-1 du code pénal) soit du fait d'une modification frauduleuse de données soit d'une entrave au bon fonctionnement d'un STAD. La loi du 24 juillet 2015 relative au renseignement a doublé les peines d'amende encourues de 75 000 euros à 150 000 euros.

Par ailleurs, depuis 2013, la détention ou la cession d'un rançongiciel, sans motif légitime, est passible des mêmes peines.

Dans le cadre des atteintes aux STAD, la circonstance aggravante de bande organisée est très souvent retenue. En effet, la commission de ces infractions requiert en principe la mise en oeuvre de différentes compétences et donc l'intervention de plusieurs personnes pour la conception, injection du virus, expédition du mail infecté, collecte de la rançon.