LES RANÇONGICIELS

Un rançongiciel (Ransomware en anglais) est un logiciel malveillant qui bloque l'accès à l'ordinateur ou aux fichiers des victimes et qui leur réclame le paiement d'une rançon pour en obtenir à nouveau l'accès. Fréquemment, ils chiffrent les fichiers se trouvant sur l'ordinateur de la victime, voire sur des serveurs qui hébergent leurs fichiers. Les victimes sont généralement infectées suite à l'ouverture d'une pièce-jointe infectée, ou après avoir cliqué sur un lien malveillant reçus dans des courriels, et parfois simplement en naviguant sur des sites Internet compromis par les cybercriminels. 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

L'objectif de ce type d'attaque commise par des organisations criminelles est d'extorquer de l'argent à la victime en échange de la promesse, pas toujours tenue, du moyen lui permettant de retrouver l'accès à ses informations.

Certaines attaques se présentant comme des rançongiciels visent à simplement saboter le système d'information de la victime pour lui faire subir des pertes d'exploitation et porter atteinte à son image, car aucun moyen de recouvrement des informations ne sera fourni à la victime et la rançon ne pourra parfois même pas être payée.

MESURES PRÉVENTIVES

- Appliquez de manière régulière et systématique les correctifs de sécurité du système d'exploitation et des logiciels installés sur votre machine.
- Mettez à jour l'antivirus et configurez le pare-feu de votre ordinateur.
- N'ouvrez pas les courriels non sollicités ou suspects.
- N'ouvrez pas les pièces jointes et ne cliquez par sur les liens provenant de chaines de messages, d'expéditeurs inconnus, ou d'un expéditeur connu mais dont la structure du message est inhabituelle ou vide.
- Ne cliquez pas sur des liens vers des sites inconnus ou non sollicités.
- En entreprise, ne téléchargez pas d'applications ou programmes qui n'ont pas été vérifiés par votre service informatique.
- Evitez 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'ouvrez pas vos courriels, et ne naviguez pas sur Internet depuis un compte ayant des droits « Administrateur ». Utilisez un compte ayant des droits « Utilisateur ».
- Lorsque vous ne vous servez plus de votre machine, éteignez la.

SI VOUS ÊTES VICTIME

- Débranchez la machine d'Internet ou du réseau informatique.
- En entreprise, alertez immédiatement votre responsable sécurité ou 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 de votre domicile ou en écrivant au procureur de la République dont vous dépendez. Faites vous au besoin assister par un avocat.
- Appliquez ou faites appliquer une méthode de désinfection lorsqu'elle existe(*). Dans le cas contraire ou en cas de doute, effectuez ou faites effectuer une restauration complète de votre ordinateur : il faut reformater le poste et réinstaller un système sain ; puis restaurer les copies de sauvegarde des fichiers perdus, lorsqu'elles sont disponibles.

LES RANÇONGICIELS

(*) ***Chaque logiciel malveillant a son propre fonctionnement et les méthodes de désinfections diffèrent selon le type de logiciel. Les sites suivants peuvent fournir des solutions dans certains cas :***

https://www.nomoreransom.org/fr/index.4html

https://stopransomware.fr/

Les infractions

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 - obligeant à une remise de fonds non volontaire.

L'article 312-1 du code pénal dispose : 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 œuvre de différentes compétences et donc l'intervention de plusieurs personnes pour la conception, injection du virus, expédition du mail infecté, collecte de la rançon.