CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES RANÇONGICIELS

Les rançongiciels (Ransomware) sont une catégorie particulière de logiciels malveillants qui bloquent l'ordinateur des internautes et réclament le paiement d'une rançon pour en obtenir à nouveau l'accès.

Depuis 2013, une variante est apparue avec des virus chiffrants ou crypto-virus (cryptolocker, cryptoDefense, cryptorBit et plus récemment locky, petya ou WannaCry). Cette forme de rançongiciels chiffre les documents se trouvant sur l'ordinateur cible, voire sur des serveurs qui hébergent les données. Les cybercriminels communiquent parfois la clé de déchiffrement une fois le paiement de la rançon effectué, mais ce n'est jamais une garantie.

Ces rançongiciels se propagent généralement :

- *par courriels dans les réseaux des entreprises, des administrations, des associations ou même des particuliers par un simple clic sur une pièce jointe ou sur un lien infectés ;*
- *par navigation sur des sites Internet qui auront été préalablement contaminés par les cyberattaquants.*

Les sites proposant des contenus pornographiques et les sites de téléchargement illicites sont souvent des vecteurs d'infections virales. Le code malveillant est injecté dans des ordinateurs dont le système d'exploitation, le navigateur Internet ou les extensions (comme « java » ou« adobe flash ») ne sont pas à jour. Aucune action ne peut plus alors être effectuée sur l'ordinateur infecté.

MESURES PRÉVENTIVES

- Appliquez de manière régulière et systématique les correctifs de sécurité du système d'exploitation et des logiciels associés
- Mettez à jour l'antivirus à jour et le pare-feu de votre ordinateur
- N'ouvrez pas les courriels ou liens non sollicités ou suspects
- N'ouvrez pas les pièces jointes provenant de chaines ou d'expéditeurs inconnus ou dont l'expéditeur est connu mais dont la structure du message est inhabituelle ou vide
- Ne cliquez pas sur des liens vers des sites inconnus ou non sollicités
- Ne télécharger pas d'applications et programmes qui n'ont pas été vérifiés par le service informatique de votre entreprise
- Evitez les sites non sûrs, hébergeant des contrefaçons, des films commerciaux en streaming, les sites pornographique qui peuvent injecter du code en cours de surf et infecter la machine
- Faites des sauvegardes régulières de votre système pour pouvoir le réinstaller dans son état d'origine au besoin
- Lorsque vous ne vous servez plus de votre machine, éteignez la

SI VOUS ÊTES VICTIME

- Débranchez la machine du réseau 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 au commissariat ou à la gendarmerie la plus proche

LES RANÇONGICIELS

Chaque logiciel malveillant a son propre fonctionnement et les méthodes de désinfections diffèrent selon le type de logiciel.
Ces sites 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'infraction d'atteinte à un système de traitement automatisé de données (STAD) pourra aussi être retenue 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.