1- Les ransomwares

Un *ransomware* ou logiciel de rançon est un logiciel qui chiffre les données d'un ordinateur et demande au propriétaire de verser un une somme d'argent en échange de la clé qui permettra de les déchiffrer. Le paiement est souvent demandé dans une monnaie virtuelle, telle que Bitcoin, afin que la transaction ne soit pas tracée et que l'identité du cybercriminel ne soit pas connue.

Pour infecter un ordinateur le pirate peut utiliser diverses techniques, notamment en rattachant le logiciel en pièce jointe d'un email, en infectant des périphériques de stockage externes ou des sites Web compromis.

Les Types de Ransomware

Il existe actuellement deux types de *ransomwares* : les *ransomwares crypto* et les *ransomwares Locker*

- Le Ransomware crypto :

Figure 1 Exemple d'interface d'un ransamware crypto {source adc-soft.com]

Le ransomware crypto est un logiciel qui a pour objectif de chiffrer les fichiers de l'ordinateur sans pour autant affecter les fonctions de celui-ci. L'utilisateur peut ouvrir sa session et naviguer mais ne peut pas ouvrir ses images, vidéos et autres fichiers.

Dans la majorité des cas, le programme comprend un compte à rebours affichant le délai de paiement et un message informant que les données seront supprimées à la fin de celui-ci.

- Le Ransomware Locker

Figure 2 Exemple d'interface d'un ransomware locker [source knowbe4.com]

Contrairement au ransomware crypto, il ne s'attaque pas aux fichiers mais empêche l'utilisateur d'accéder à sa session, ou désactive partiellement les fonctions des périphériques. Comme la version crypto, le Locker émet également une demande de rançon en échange de la clé de chiffrement.

Exemples de Ransomware :

O Wannacry : aussi connu sous le nom Wannacrypt, il est apparu en mai 2017 en infectant plus de 300 000 ordinateurs dans plus de 150 pays. Elle est considérée comme étant la plus grande attaque à rançon de l'histoire d'internet touchant de grandes organisations telques Vodafone, FedEx, Renault, Telefónica, le National Health Service, le Centre hospitalier universitaire de Liège, le ministère de l'Intérieur russe ou encore la Deutsche Bahn.

O Locky : aparu en mi-février 2016, il infecte les systèmes via des pièces jointes Microsoft Word contenant des macros malveillantes. Une autre mise à jour de Locky, en juillet 2016, permettait à la souche de chiffrer des fichiers hors connexion, ce qui

signifie que le fait d'éteindre un ordinateur dans le cadre d'un réseau plus grand ne permettrait pas d'éviter l'infection d'autres ordinateurs. Locky est actuellement l'une des trois plus grandes menaces de ransomware qui a essentiel affectée le secteur de la santé.

O Cryptolocker : il a été le ransomware le plus rentable, entre septembre et décembre 2013, il a infecté plus de 250, 000 ordinateurs rapportant plus de 3 millions de dollars à son créateur. Par la suite, son modèle de cryptage a été analysé et un outil en ligne est maintenant disponible pour récupérer les fichiers cryptés compromis par CryptoLocker.

O Cerber : Le ransomware Cerber est un ransomware-as-a-service (RaaS), c'est-à-dire que le hacker en diffuse des licences sur Internet et partage la rançon avec le développeur.

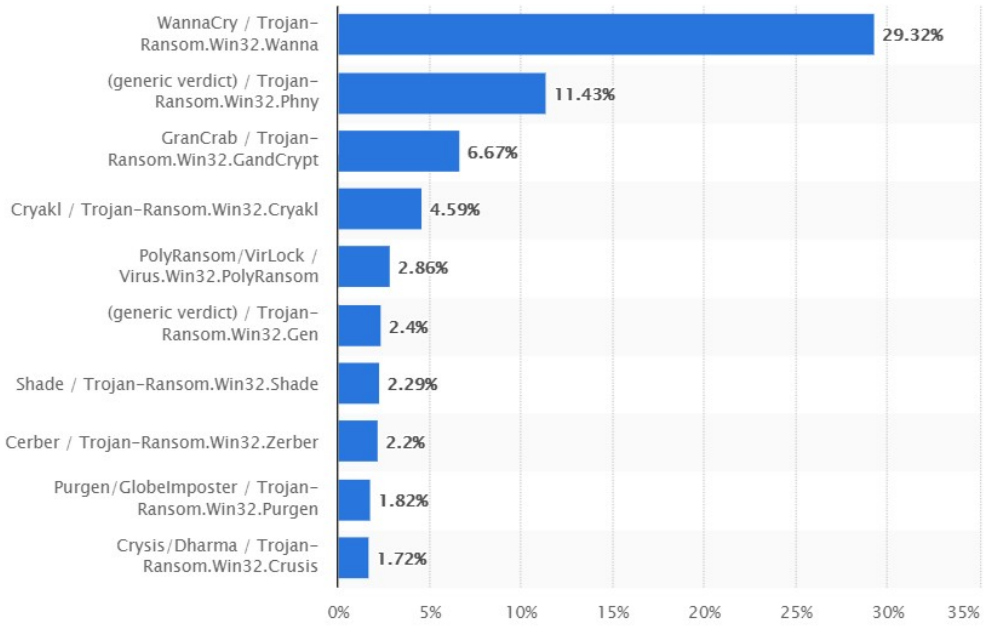

Figure 3Familles les plus courantes de ransomware en 2018

- **Techniques de prévention contre les ransomwares**

Les ransomwares sont généralement installés suite à un clique d'un utilisateur sur un lien malveillant, pour prévenir des ransomwares plusieurs bonnes pratiques peuvent être partagées aux utilisateurs internes et externe du SI :

- Ne pas cliquer sur un lien malveillant :

  Si un utilisateur reçoit un email contenant un lien qui lui semble malveillant, il devrait contacter le responsable de la sécurité du système informatique avant de prendre la moindre décision. Aussi il faut que les utilisateurs évitent d'accéder à des sites qui proposent des vidéos ou films en *streaming*, ces sites sont généralement remplis de liens malveillants.

- Ne pas ouvrir une pièce jointe suspecte

  Un autre moyen permettant aux ransomwares de s'installer sur une machine consiste à joindre le logiciel malveillant à une pièce d'un email.

  Les utilisateurs ne doivent pas ouvrir des pièces jointes d'emails d'expéditeurs en qui ils n'ont pas confiance.

- Lancer des téléchargements provenant de site de confiance

  Internet aujourd'hui contient énormément de sites WEB malveillants, il faut toujours s'assurer d'être sur le bon site en vérifiant l'URL avant de lancer un téléchargement et éviter de lancer des téléchargements de sites inconnus.

- Ne jamais connecter un périphérique de stockage inconnu

  Si un utilisateur retrouve une clé USB ou un autre périphérique de stockage de données abandonnée, il doit en informer le RSSI et à aucun moment il ne doit le connecter sur une machine car il pourrait être infecté.

- Effectuer des mises à jour des logiciels et systèmes d'exploitation

  Les mises à jour permettent ne remédier à des failles de sécurité mais aussi à des erreurs sur le SI, lorsque vous exécutez une mise à jour, vous vous assurez de bénéficier des derniers correctifs de sécurité, ce qui empêche les cybercriminels d'exploiter les vulnérabilités de votre logiciel.

- Effectuer des sauvegardes

  La sauvegarde de données reste la méthode la plus efficace pour récupérer les données en cas d'attaque par ransomwares, car il se peut qu'il soit impossible de déchiffrer les données présentes sur l'ordinateur victime.