Les ransomwares

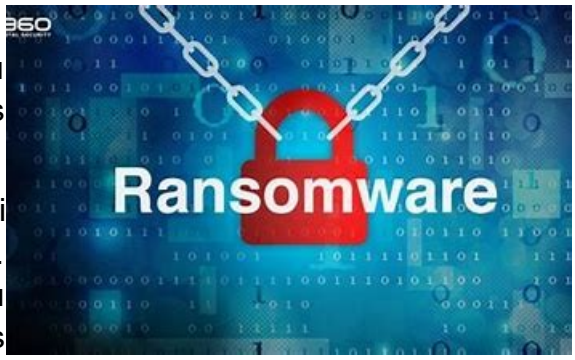
Sommaire

1.Les Ransomware :

1.1.Définition :

Un ransomware est un type de malware, ou programme malveillant, qui prend en otage des fichiers et parfois des ordinateurs ou des appareils mobiles entiers. On peut définir un ransomware par ce comportement : les pirates demandent une rançon en échange de la restitution de l'accès ou du déchiffrement de vos fichiers.

1.2.Les risques :



Les ransomwares sont des attaques qui ont pour but de bloquer les fonctionnalités du système ou de voler des données confidentielles qui sont ensuite utilisées afin d'obtenir des rançons

Ces attaques constituent un danger énorme aussi bien pour les entreprises que pour le monde entier. L'objectif de chaque attaque diffère en fonction du type de programme employé.Certains programmes permettent de bloqué le système infecté à distance (ransomware Locker), pendant que d'autres se chargent de chiffrer les fichiers individuels (ransomware Crypto). Dans l'un ou l'autre des cas, les conséquences engendrées ne sont pas moindres.

1.3.Types d'attaques :

Les ransomwares font partis d'une méthode d'attaque appelé « Le cheval de troie ».
Il ne se duplique pas contrairement à un virus, il s'exécute au moment ou on ouvre un fichier qu'on peut recevoir par mail. Ce qui laissera l'auteur de cette attaque avec des portes ouverte sur votre PC

1.Ransomware Locker :

Les ransomwares Locker. Ce type d'applications malveillantes bloque les fonctions de base de l'ordinateur. Par exemple, l'accès au bureau peut vous être refusé alors que la souris et le clavier sont partiellement désactivés.

2.Ransomware Crypto :

Les ransomwares Locker. Ce type d'applications malveillantes bloque les fonctions de base de l'ordinateur. Par exemple, l'accès au bureau peut vous être refusé alors que la souris et le clavier sont partiellement désactivés.

2.Protections :

2.1.Comment être infecté :

Le rançongiciel est un logiciel malveillant qui chiffre vos fichiers ou vous empêche d'utiliser votre ordinateur jusqu'à ce que vous payez une somme d'argent (rançon) pour les déverrouiller. Si votre ordinateur est connecté à un réseau, le rançongiciel peut également se propager vers d'autres ordinateurs ou périphériques de stockage sur le réseau.

Vous pouvez être infecté par un rançongiciel de l'une des façons suivantes :

1. En visitant les sites web dangereux, suspects ou frauduleux.

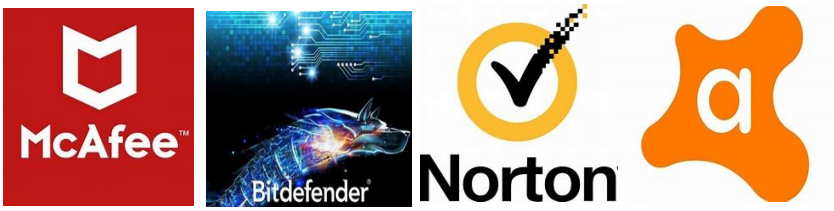
2. En ouvrant des fichiers en pièce jointe que vous n'attendiez pas ou provenant de personnes que vous ne connaissez pas.

3. En ouvrant des liens malveillants ou corrompus dans les e-mails, Facebook, Twitter et d'autres publication de réseaux sociaux, ou dans des sessions de conversation instantanée ou des conversations par SMS.

2.2.Comment se protéger :

- Il faut aussi installer un antivirus performant comme :
  (sur windows) :

  1. Avast
  2. Bitdefender
  3. Norton
  4. McAfee



  (sur macOS) :

  1. Intego

- Dès qu'une mise à jour de logiciel ou alors driver est disponible, il faut impérativement les effectuer pour éviter les failles de sécurité.

- Faire très attention aux mails que nous pouvons recevoir, ils peuvent contenir des programmes malvaillants après exécution d'un fichier (généralement sous word)

3.Conduite a tenir :

1. En cas d’attaque par ransomware, il ne faut absolument pas payer la rançon. Une fois la rançon payer le pirate peut ne pas vous redonner accès a vos données.

2. Prévenir le service informatique de l’entreprise ou alors contacter un informaticiens capable de prendre la main sur le PC

3. Alors ce qu’il est conseillé de faire est d’effectuer une réinitialisation du système. Si il n’y a vraiment aucun accès aux paramètres du PC, utilisez les disques d’installation ou clés USB sur lesquels votre système d’exploitation est sauvegardé.

4.Exemple d’attaque :

En Janvier 2020 une attaque par ransomware à visée l’entreprise Travalex, qui a été contrainte de mettre hors service tous ses systèmes informatiques. En conséquence, l'entreprise a dû mettre hors service ses sites Web dans 30 pays.
Un groupe de pirates informatiques appelé Sodinokibi était à l'origine de l'attaque, réclamant 6 millions de dollars à Travelex. Le groupe à menacé Travalex de supprimer toute les données et de doubler la rançon tout les 2 jours. Travelex aurait versé au groupe près de 2,3 millions de dollars en bitcoins et rétabli ses systèmes en ligne après deux semaines d'interruption.

Source : Top Attaques Ransomware (kaspersky.fr)