

Qu'est-ce qu'un rançongiciel?

Un rançongiciel est un type de maliciel qui retient vos données ou vos systèmes en otage. Un cybercriminel peut utiliser un rançongiciel pour verrouiller un appareil, un réseau ou un serveur, et bloquer l'accès aux données jusqu'à ce que la victime paie une rançon. En général, le paiement se fait en Bitcoin de façon à ne pas être retracé par la police.



SYSTÈME DE DISTRIBUTION DU TRAFIC

Dans ce scénario de rançongiciel, le trafic d'un site Web est redirigé vers un site Web qui héberge une trousse d'exploitation. Souvent, la redirection se fait via une fenêtre surgissante ou une publicité malveillante. La trousse d'exploitation sert à identifier les points faibles de l'ordinateur avant d'installer le rançongiciel.

BLOQUEUR

Un rançongiciel de type bloqueur est un maliciel qui bloque l'accès de l'utilisateur au système et permet aux cybercriminels de prendre le contrôle de l'appareil infiltré jusqu'à ce que la rançon soit payée. Tout ce que l'utilisateur voit, c'est une page d'instructions contenant les modes de paiement.

AUTO-PROPAGATION

Ce type de rançongiciel se propage à travers un système infecté et attaque tout ordinateur ou appareil connecté au réseau partagé.

CHIFFREUR

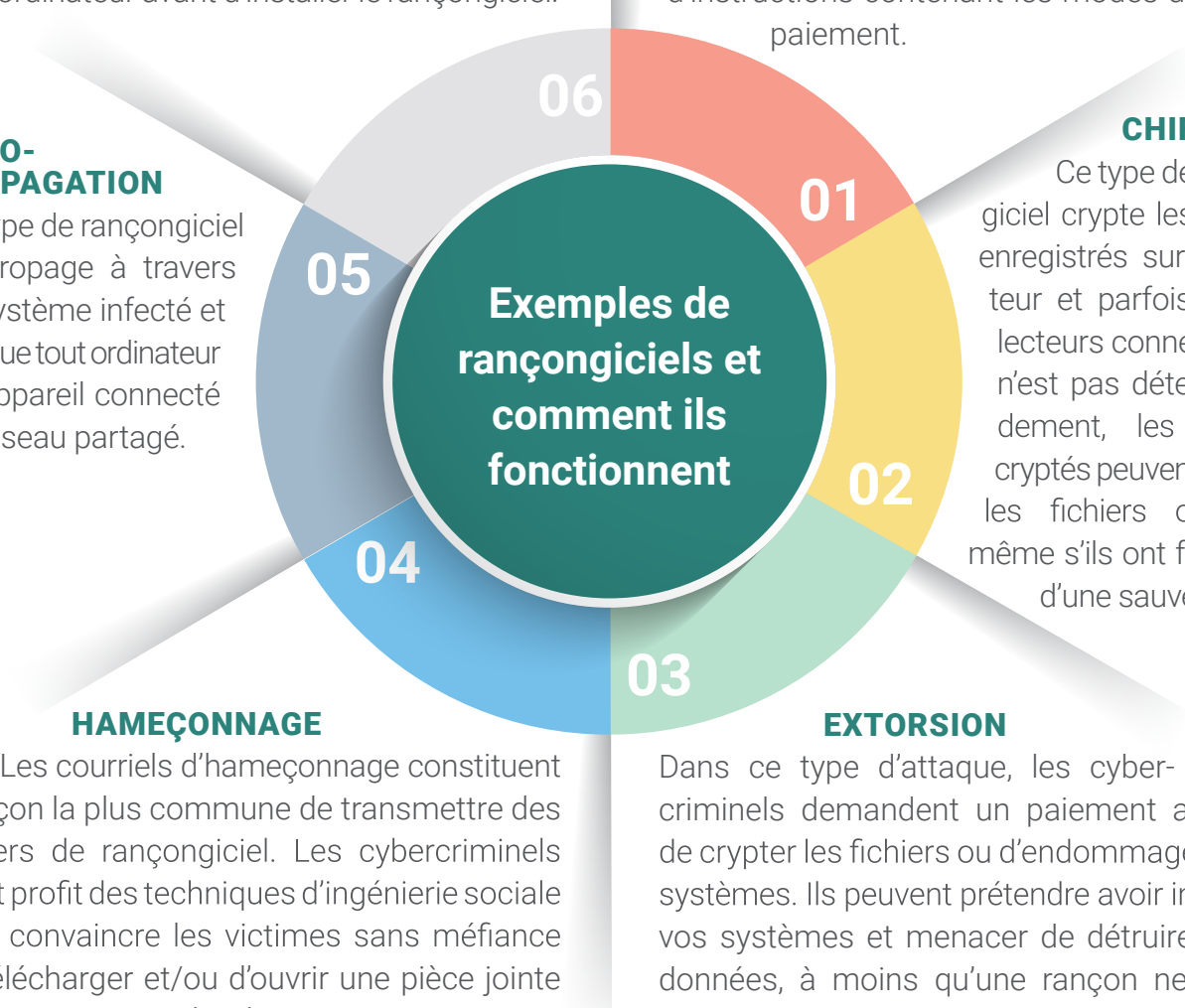
Ce type de rançongiciel crypte les fichiers enregistrés sur l'ordinateur et parfois sur les lecteurs connectés. S'il n'est pas détecté rapidement, les fichiers cryptés peuvent écraser les fichiers originaux, même s'ils ont fait l'objet d'une sauvegarde.

HAMEÇONNAGE

Les courriels d'hameçonnage constituent la façon la plus commune de transmettre des fichiers de rançongiciel. Les cybercriminels tirent profit des techniques d'ingénierie sociale pour convaincre les victimes sans méfiance de télécharger et/ou d'ouvrir une pièce jointe qui contient un maliciel.

EXTORSION

Dans ce type d'attaque, les cybercriminels demandent un paiement avant de crypter les fichiers ou d'endommager les systèmes. Ils peuvent prétendre avoir infiltré vos systèmes et menacer de détruire vos données, à moins qu'une rançon ne soit versée.



Qui peut être la cible d'un rançongiciel?

Tout type d'entreprise, de gouvernement, d'organisation ou d'individu peut être la cible d'une attaque par rançongiciel. Les cybercriminels cherchent des victimes qui sont prêtes à payer une rançon pour récupérer l'accès à leur appareil, réseau ou serveur, ainsi qu'aux données qu'ils contiennent. Pour cette raison, il est essentiel que tous vos employés soient en mesure de détecter et d'éviter ce type de cybermenace.

