Cyberattaques, l'exemple du rançongiciel

vendredi 6 février 2015, par lpe

Le rançongiciel (ransomware), c'est un programme malveillant qui s'installe sur un ordinateur et bloque l'accès aux données
et au système d'exploitation. Le propriétaire ne peut plus utiliser son ordinateur, même après un redémarrage.

Depuis quelques années, des attaques se propagent à l'aide de rançongiciels. Les programmes usités par les pirates sont particulièrement efficaces et bloquent totalement les ordinateurs des victimes.
Cette attaque est accompagnée d'une demande de rançon au propriétaire de l'ordinateur, contre le déblocage du code malveillant.

Il ne faut pas payer cette rançon car, de toute façon, le pirate ne vous enverra jamais de solution palliative à ce problème. La seule possibilité est souvent une réinstallation complète du système d'exploitation.

Ce type d'attaque particulièrement sophistiquée relève d'une escroquerie du crime organisé, principalement, venant des pays de l'est. Le rançongiciel est un faux avertissement d'une autorité gouvernementale (gendarmerie, police, hadopi), signalant que l'ordinateur infecté serait utilisé à des fins illégales par son propriétaire (réseaux peer to peer, films pornographiques, copies de logiciels etc.). Le but ultime des pirates étant de faire payer une forte rançon à la victime mis sous pression par de telles accusations.

Le modus opérandi de ces hackers est basé sur la naïveté et la curiosité des victimes :
- Des robots informatiques observent les failles de sécurité des ordinateurs afin de déterminer le maillon faible des matériels numériques observés. Dès qu'un utilisateur reçoit une pièce jointe ou en visitant les sites énoncés ci-dessous puis clique sur un lien malveillant proposé sur ce type de site, la contamination s'active ''trop tard, le ver est dans le fruit''. Le système d'exploitation de l'ordinateur est bloqué.
- La contamination se réalise à l'aide de publicité, de pièces jointes dans les courriels, et lors de la visite sur les réseaux sociaux et sites de pirates
informatiques.

Il existe plusieurs variantes de rançongiciels toutes plus impressionnantes les unes que les autres. Sur certains écrans apparaissent l'adresse IP de la machine infectée ainsi que le visage (webcam) de l'utilisateur qui se croit surveillé en temps réel.

Précautions : Les quelques conseils ci-dessous vous permettront de limiter grandement le risque rançongiciel :
- Sensibiliser les utilisateurs à ce type d'attaque sournoise.
- Sauvegarder régulièrement vos données sur des supports hors ligne.
- Utiliser des antiviraux et les applicatifs à jour (système d'exploitation et logiciels).
- Sectoriser l'accès aux données sur le serveur d'une entreprise.
- Attention aux pièces jointes sur un courrier douteux. Un simple clic sur une pièce jointe vérolée engendrera automatiquement l'installation
du programme malveillant.

Réactions :
Lorsqu'un ordinateur est infecté, il est nécessaire d'appliquer urgemment les éléments ci-dessous :
- Important : Ne pas payer la rançon car le pirate ne vous donnera jamais le code de déblocage du logiciel malveillant.
- Isoler le, ou les postes victimes.
- Si possible, alertez vos correspondants récents sur le risque avéré s'ils reçoivent un message avec pièce jointe, identique, à celui qui vous a
infecté.
- Faire appel à une personne aux ressources qualifiées pour nettoyer votre ordinateur et réinstaller vos sauvegardes récentes
(système d'exploitation et logiciels).
- Déposer une plainte est judicieux afin de permettre aux forces de l'ordre
(police - gendarmerie) de remonter aux sources de l'attaque et de sensibiliser les utilisateurs à ces applications malveillantes.

Jean-Michel Lathière, adjudant chef au sein de l'antenne intelligence économique de la Région de gendarmerie en Poitou-Charentes.