Combattre les Ransomwares avec Kaspersky Lab

Maxime - 2020-02-17 - Kaspersky

Les Ransomwares sont une variété de malwares qui, une fois qu'ils ont infecté un ordinateur, affirment en avoir chiffré les données avant de bloquer l'ordinateur de la victime.
Le malware informe ensuite l'utilisateur infecté qu'il ou elle doit payer une rançon afin de déverrouiller ses fichiers.

Vecteurs d'infection – Protection
Les vecteurs d'infections possibles sont :

- Mails (Phishing)
- Supports amovibles
- Sites Web
- Sessions Terminal

L'infection peut se produire lorsque :

- La solution de sécurité de l'ordinateur n'est pas à jour.
- L'installation est autorisée en dépit des avertissements des solutions de sécurités qu'un programme spécifique peut être malveillant.
- L'utilisateur a défini l'analyse heuristique des fichiers au réglage minimum.
- La configuration de l'antivirus n'est pas protégée par un mot de passe.
- Les technologies proactives ne sont pas utilisées. (KSN, Défense Proactive / System Watcher)
- La configuration du module de contrôle de l'activité des applications n'est pas au point

Recommandations et Best practices :

- Utiliser une solution Kaspersky Endpoint Security 8/10 à jour
- Mettre à jour quotidiennement les bases de signatures virales.
- Respecter les règles de base de la sécurité du réseau en accordant une attention particulière à tous les fichiers provenant de sources inconnues ou téléchargés à partir de sites Web suspects.
- Procéder à l'installation et l'utilisation uniquement d'applications familières de sources fiables telles que le site officiel du développeur.
- Gardez votre produit de sécurité activé en le protégeant par un mot de passe.
- Ne pas modifier la configuration des différents composants de détection de logiciels malveillants et le niveau de protection recommandé sauf si c'est absolument nécessaire.
- Activer les technologies proactives telles KSN (Kaspersky Security Network) et le module System Watcher incluant la Défense proactive.

- Protection contre les ransomwares à l'aide du module de contrôle de l'activité des applications : http://support.kaspersky.com/fr/10905

Pièces à collecter pour le laboratoire Kaspersky

- Les éléments collectés à l'aide de l'outil Kaspersky Log Utility : http://support.kaspersky.com/us/11071#block1
- L'exemplaire du/des exécutables malicieux identifiés compressés dans une archive protégée par le mot de passe infected.
- La plupart des codes malicieux de ce type sont généralement supprimés du poste automatiquement (routine intégré dans le code). Ainsi, nous vous conseillons de regarder les fichiers exécutables supprimés récemment.

Des outils de type « gratuit » le permettent (exemple : Recuva = http://www.piriform.com/recuva).

- Un fichier chiffré et la version originale du fichier (si vous avez une sauvegarde des fichiers).
- Le répertoire des fichiers chiffrés (exemple Mes Documents, Mon Ordinateur…).
- Le dump à chaud de la mémoire lorsque le chiffrement est en cours d'exécution à l'aide d'outils tels que « DumpIT » disponible ci-dessous : http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/

La procédure de génération du dump avec DumpIt est la suivante :

• Télécharger DumpIt : http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7
• Exécuter l'exécutable depuis le poste infecté et lors de la routine de chiffrement du code malicieux. Un fichier <nom de fichier>.raw est créé :
• Compresser le fichier et le faire parvenir à l'ingénieur pour analyse.

- Dans le cas où le module System Watcher de KES8/10 est active dans la partie Endpoint Protection, collectez les fichiers malicieux qui ont été placés dans le répertoire de backup du module "System Watcher" (C:\ProgramData\Kaspersky Lab\KES10\SysWHist\file_cache) Compressez ces fichiers dans une archive protégée par mot de passe.
- Collectez également tout le contenu de ce répertoire dans une archive protégée par mot de passe : C:\ProgramData\Kaspersky Lab\KES10\QB\

Joignez le fichier clé de licence (.KEY) utilisé sur le poste client infecté dont les analystes Kaspersky auront besoin pour la gestion des fichiers en quarantaine.

Les fichiers doivent être transmis dans une unique archive (compressée avec WinRar, 7 Zip…).

Dans le cas où l'archive fait plus de 50 MB, vous pouvez l'uploader sur un site permettant le partage de fichiers, puis leur faire parvenir le lien de téléchargement.