Quelques pistes en prévention ou en curation d’attaque par ransomwares

	Quelques pistes en prévention ou en curation d’attaque par ransomwares

Un de vos clients est victime d'un ransomware. Cryptolocker, Cryptowall, Supercrypt, TeslaCrypt, … Peut importe le malware, le résultat est à peu prêt le même. Ses fichiers sont cryptés, et l'impact est énorme. Dans l'urgence, il convient de procéder correctement, en prenant certaines précautions. Je vais donc ici vous donner quelques pistes (un peu en vrac) afin de traiter au mieux le problème.

Sauvegarde

J'imagine que si vous consultez cet article, aucune sauvegarde de votre client n'est exploitable. Sinon, vous l'auriez remontée.
Cependant, avant d'envisager toute action sur le/les systèmes infectés, pensez à procéder à une sauvegarde. Je recommande d'arrêter immédiatement ces systèmes infectés. Ensuite, qu'il s'agisse d'un serveur, ou d'un simple client, clonez le disque dur.
Pour cela, effectuez un clone en mode hors ligne, avec un de ces outils par exemple : Acronis, Veeam, AOMEI.
Ca vous permettra d'effectuer les tests que vous voulez sur le clone, sans aucun risque.

Lister les fichiers cryptés

Un outil bien pratique permet de lister les fichiers cryptés par Cryptowall. En effet, cette infection stocke la liste des fichiers qu'elle crypte dans le registre. L'outil ListCWall permet de localiser et utiliser ces infos afin de vous sortir une liste des fichiers, et permet aussi de les exporter afin de les stocker par exemple sur un média externe avant de formater la machine si besoin.

Utilitaires de décryptage

Ce qu'il faut retenir de ce paragraphe, ce n'est pas autant la liste des outils (non exhaustive) que je vous propose, mais que de tels outils voient le jour périodiquement. Pensez à regarder du côté des éditeurs d'antivirus (ou sur Tech2Tech!!), si un nouvel outil existe concernant l'infection que vous avez à traiter en particulier. En effet, suite à des enquêtes internationales, parfois, des réseaux tombent. Et lorsque les services en charge de ces enquêtes découvrent un lot de clés de cryptages, les éditeurs d'antivirus peuvent les exploiter afin de les intégrer dans des outils de décryptage. Pas sur que ca fonctionne donc (si la clé utilisée ne fait pas partie de celles qui ont été découvertes) mais vous pouvez le tenter…
On peut lister par exemple :
RectorDecryptor chez Kaspersky (pour le ransomware Rector)
XoristDecryptor chez Kaspersky (pour le ransomware Xorist/Vandev)
ScatterDecryptor chez Kaspersky (pour le ransomware Scatter)
ScraperDecryptor chez Kaspersky (pour le ransomware Scraper)
RakhniDecryptor chez Kaspersky (pour le ransomware Rakhni)
Ransomware Decryptor chez Kaspersky (pour le ransomware Coinvault/Bitcryptor)
Decryptor 0-1.3 chez Bitdefender (pour le ransomware Linux.Encoder.1)
DecryptCryptoLocker par FireEye et Fox IT (pour le ransomware CryptoLocker)
TeslaDecrypt par Cisco Talos Security Intelligence (pour le ransomware TeslaCrypt)

Récupérer les fichiers

A ma connaissance, si vous n'avez pas de sauvegardes, et que le ransomware n'a pas d'outil de décryptage dédié ayant été élaboré, il y a peu de chances de retrouver les fichiers.
Cependant, deux pistes peuvent s'avérer intéressantes :

Shadow Volume Copies

Les shadow copies (service de clichés instantanés), peuvent s'avérer utiles dans le cas d'un ransomware. Cependant, il faut déjà que le service soit activé et configurée correctement. Ensuite, la majorité des ransomware un peu élaborés et récents désactivent ce service, et vont effacer les snapshots déjà présents. S'ils s'avèrent utilisables, le logiciel Shadow Explorer sera pratique pour récupérer les fichiers.

Récupération de données

Il semblerait que, dans le cas de certains ransomware, les fichiers soient copiés, cryptés, puis supprimés. Il serait alors envisageable, si la machine est arrêtée au plus vite, de récupérer des fichiers à l'aide d'un utilitaire de récupération de données.
Pour cela, clonez d'abord le disque par précaution, en mode hors ligne (Live CD).

Se protéger des ransomwares

Plusieurs éditeurs de solutions de sécurité proposent des utilitaires plus ou moins élaborés afin de se protéger contre un cryptage de données.
Il y a d'abord une approche qui consiste à interdire le lancement d'exécutables situés dans %APPDATA%. C'est en effet un mode de fonctionnement courant de ce type de malwares. Cette fonction est proposée par Bitdefender à travers son outil gratuit Anti-Cryptowall. Personnellement cet utilitaire ne m'a pas vraiment convaincu lorsque je l'ai essayé, puisque j'ai pu lancé des exe situés dans %APPDATA%…
CryptoPrevent, utilitaire développé par Foolish IT permet de se prémunir d'une attaque par un CryptoLocker. Cependant, la version gratuite nécessite des mises à jours manuelles visiblement. Voyez plutôt vos besoins sur les différentes versions commerciales.
BitDefender a intégré dans sa version grand public 2016 un moteur d'analyse de cryptage. Le but est d'analyser en temps réel une éventuelle activité de cryptage sur la machine, et de la stopper. Cette fonction sera intégrée dans les antivirus pro maximum en début d'année 2017.
Pour ma part, je suis distributeur des solutions Panda Security Cloud. Et un outil a été mis au point durant l'été : Adaptive Defense 360. Venant en renfort de n'importe quel antivirus, ce produit permet de bloquer tous les logiciels que l'entreprise n'a pas décidé explicitement de laisser fonctionner sur son parc. Il en résulte une protection quasi parfaite, même si ca a un coût. Et comme il faut bien manger, je me fais au passage une petite pub : n'hésitez pas à me contacter si vous désirez vous équiper de cette solution!
Ce ne sont évidement que des exemples, non exhaustifs. Mais ils traduisent la diversité des solutions élaborées afin de contrer les ransomwares et cryptolockers, qui sévissent actuellement de manière dramatique.

Réagissez à cet article
Source : http://www.tech2tech.fr/ransomware-avec-cryptage-quelques-pistes/