Aide-mémoire rançongiciels

Les chevaux de Troie verrouillant les données, appelés aussi rançongiciels (ransomware), appartiennent à une famille particulière de logiciels malveillants (maliciels) qui chiffrent les données sur l'ordinateur de la victime ainsi que sur les lecteurs réseau auxquels cet ordinateur est relié, ce qui les rend inutilisables pour la victime. Les rançongiciels font alors afficher un écran verrouillé demandant à la victime de payer une certaine somme sous forme de bitcoins (une monnaie virtuelle) pour déverrouiller les données. La liste des logiciels de chantage ne cesse de s'allonger et les versions actuelles ont un potentiel de nuisance bien plus élevé que les premières versions, lesquelles se contentaient de bloquer l'écran. Ces chevaux de Troie accèdent à l'ordinateur par le biais de courriels infectés ou de sites Internet piratés.

Incidences et risqué

- Données de l'ordinateur rendues inutilisables
- Dommages financiers en cas de paiement d'une rançon

Mesures préventives

- Veillez à effectuer des sauvegardes régulières de vos données importantes sur un support externe (par ex. un disque dur externe). Après la sauvegarde, veillez à déconnecter de l'ordinateur le support contenant les données sauvegardées, sans quoi ces données pourront également être verrouillées et rendues inutilisables en cas d'infection de l'ordinateur par un rançongiciel.
- Il convient de toujours maintenir à jour son système d'exploitation et toutes les applications installées sur son ordinateur (par ex. Adobe Reader, Adobe Flash, Sun Java), de manière automatique lorsque cela est possible.
- Il convient d'être toujours extrêmement prudent en présence de courriels suspects, inattendus ou provenant d'un expéditeur inconnu: ne suivez pas les recommandations figurant dans le texte, ne cliquez pas sur les liens indiqués et n'ouvrez pas les documents joints au courriel.
- Veillez à ce que votre antivirus soit à jour. Si vous disposez d'un antivirus payant, pensez à prolonger l'abonnement chaque année, sans quoi l'antivirus sera inutile.
- Un pare-feu (firewall) personnel doit être installé et régulièrement mis à jour.
- Depuis le début du mois de mars 2016, abuse.ch met à la disposition de tous les utilisateurs d'Internet un traqueur capable de reconnaître différentes familles de rançongiciels, ainsi que des listes de blocage.

Mesures après l'infection de l'ordinateur

- En cas d'infection, il est recommandé de déconnecter immédiatement l'ordinateur de tous les réseaux. Une réinstallation du système et un changement de tous les mots de passes sont bien entendu nécessaires.
- Une fois ces mesures prises, il sera possible de restaurer les données à partir de copies de sauvegarde si ces dernières existent. S'il n'existe aucune sauvegarde, nous recommandons de conserver les fichiers chiffrés en vue d'une éventuelle solution future qui pourrait permettre de les déchiffrer.
- En tous les cas, MELANI conseille à la victime de signaler l'incident au Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) et de porter plainte auprès des services de police locaux.
- Ne cédez pas à l'extorsion car, en payant la rançon, vous participez au financement de l'activité des criminels et leur permettez d'améliorer l'efficacité de leurs prochaines attaques. De plus, il n'existe aucune garantie que les criminels respecteront leur engagement et vous enverront réellement la clé vous permettant de récupérer vos données.

Mesures pour les PME

MELANI suggère aux entreprises d'appliquer les mesures supplémentaires suivantes:

- Vous pouvez renforcer la protection de votre infrastructure informatique contre les maliciels (tels que les rançongiciels) en utilisant le programme Windows AppLocker[1]. Celui-ci vous permettra de définir les programmes qui pourront être ouverts sur les ordinateurs au sein de votre entreprise.
- Le programme EMET de Microsoft (Enhanced Mitigation Experience Toolkit)[2] permet d'éviter que les failles de sécurité aussi bien connues qu'inconnues de logiciels exploités dans votre entreprise ne puissent favoriser l'installation d'un maliciel.
- Bloquez la réception de courriels contenant des fichiers dangereux sur votre passerelle de messagerie. Sont dangereux notamment les fichiers.

.js (JavaScript)
.jar (Java)
.bat (Batch file
.exe (Windows executable
.cpl (Control Panel)
.scr (Screensaver)
.com (COM file)
.pif (Program Information File)
.vbs (Visual Basic Script)
.ps1 (Windows PowerShell)

Veillez à ce que ces fichiers soient également bloqués lorsqu'ils sont envoyés dans un fichier d'archive tel qu'un fichier ZIP ou RAR ou dans un fichier crypté (par ex. un fichier ZIP protégé par un mot de passe).

Par ailleurs, il faudrait bloquer tous les fichiers joints contenant des macros (par ex. Word, Excel ou PowerPoint contenant des macros).

[1] https://technet.microsoft.com/en-us/library/dd759117.aspx
[2] https://support.microsoft.com/en-us/kb/2458544

Consultez le document de MELANI «Sécurité informatique: aide-mémoire pour les PME» ainsi que le programme en dix points visant à accroître la sécurité informatique sur le portail PME de la Confédération «Sécuriser son infrastructure informatique».

Sécurité informatique: aide-mémoire pour les PME:
https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

Sécuriser son infrastructure électronique:
https://www.kmu.admin.ch/kmu/fr/home/savoir-pratique/gestion-pme/infrastructure-ti/infrastructure-technologie-information-ti/infrastructure-securite-ti.html

Vous trouverez cet aide-mémoire également en ligne à l'adresse suivante :
https://www.melani.admin.ch/ransomware