COMPLÉMENT D'INFORMATION

Ransomware ou rançongiciel

Comportement classique : un pop-up apparait, souvent provenant supposément du FBI, de la GRC ou d'un autre service de police ou agence gouvernementale, vous avisant qu'une activité illégale a été détectée en provenance de votre ordinateur et que votre ordinateur sera maintenant bloqué jusqu'à ce qu'une amende ait été payée.

Autre possibilité, un message apparait, vous informant que vos fichiers ont été cryptés ou votre ordinateur verrouillé et que vous devrez payer un montant afin de récupérer le mot de passe pouvant les débloquer.

Point d'entrée : historiquement, ce type de malware (logiciel indésirable) était « attrapé » sur des sites pornographiques et de piratage (crack pour débloquer des jeux ou logiciels piratés). De nos jours, la majorité provient de courriels ayant une pièce jointe et plus récemment, de pop-up provenant de sites infectés (publicités, promotions du type « vous avez gagné un iPad… ») ou d'applications compromises ou provenant de sources peu fiables… Des versions ont même été découvertes sur l'App Store ce printemps attachées à une application…

Mode d'opération : dès son activation sur un ordinateur, le logiciel (virus) s'attaque à tous les fichiers auxquels il peut accéder, que ce soit sur les lecteurs locaux, les lecteurs attachés (USB) ou les lecteurs réseaux et crypte ces fichiers avec une clé de codage spécifique. Dans certains cas, il est même possible que les fichiers hébergés dans un espace de stockage dans le nuage soient touchés. Le virus est conçu spécialement pour se concentrer sur les fichiers personnels : les documents Microsoft Word, les photos, vidéos, musique, etc.

Détection : la détection de ce type d'infection est très difficile par les antivirus en raison de leur fonctionnement : leur activité est souvent perçue tout simplement comme un usager lisant puis refermant des fichiers auxquels il a légitimement accès. L'antivirus recherche des modèles ou signatures de virus, mais les fichiers générés ne présentent pas ce type de signatures, il s'agit uniquement de fichiers standards, mais cryptés. Le signal le plus évident reste souvent un message qui apparait à l'usager infecté l'informant que ses fichiers sont cryptés et les modalités de paiement permettant de les décrypter. Le message est parfois accompagné d'un décompte indiquant le temps restant pour payer la rançon avant la destruction de la clé rendant les données irrécupérables : les personnes ont souvent une moins bonne capacité de réflexion quand ils sont confrontés à une limite de temps. D'autres signes permettant la détection sont un message de fichier illisible à l'ouverture d'un fichier, la présence de fichiers ayant l'une des extensions répertoriées plus bas ou la présence de l'un des fichiers énumérés plus bas dans un répertoire.

Récupération : sauf dans le cas d'anciennes variantes du processus de cryptage, il n'existe en général que 2 méthodes permettant de récupérer les données : restaurer une sauvegarde ou payer la rançon. De plus, la rançon exigée est la plupart du temps peu élevée (environ 300 $ ou moins pour un ordinateur personnel) ce qui porte souvent la personne affectée à préférer payer plutôt que de subir la perte de ses données ou à entreprendre un long processus (tentatives de décryptages à partir d'un second ordinateur, plainte aux autorités, etc.) dans l'espoir de récupérer les données sans débourser. Quelques utilitaires (chez Cisco et Kaspersky entre autres) permettent de décrypter soi-même les fichiers lorsqu'ils ont été cryptés avec une des premières versions du virus, mais sont inefficaces avec les nouvelles générations. Elles exigent également que vous ayez au moins une copie non cryptée de l'un des fichiers cryptés afin d'extraire la clé en comparant les deux fichiers.

Protection : toujours être extrêmement prudent lors de l'ouverture de pièces jointes, même en provenance de personnes connues (l'envoi de copie du malware par courriel aux contacts de la personne infectée est encore parfois utilisé) : dans le cas de fichiers au nom douteux ou quand il vous apparait curieux de recevoir un fichier d'une certaine personne, ne pas l'ouvrir sans avoir vérifié auprès de la personne si elle a vraiment expédié de façon volontaire le message et le fichier.

À la maison, éviter de télécharger des applications ailleurs qu'à partir de sites « sérieux » par exemple le site officiel du concepteur. Éviter tout téléchargement lancé à partir d'un courriel, surtout quand la source est inconnue ou peu connue (des attaques lancées à partir d'un lien vers une facture ont été recensées).

Lors de l'apparition de fenêtres pop-up, toujours utiliser le x dans le coin supérieur pour la fermer, éviter d'utiliser les boutons inclus dans la fenêtre. Lorsque le X ne fonctionne pas, utiliser les touches CTL-ALT-DEL et fermer complètement l'application du navigateur.

En cas d'infection confirmée, éteindre l'ordinateur au plus vite (couper l'alimentation, touche Power de façon continue pour un appareil portatif ou retrait de la batterie) et déconnecter l'ordinateur du réseau et de tout périphérique externe (disque USB, clé, etc.). Effectuer des sauvegardes régulières de vos données.

À la maison, toujours utiliser un antivirus détectant également les applications ou accompagné d'un anti-malware et s'assurer que ceux-ci sont à jour. Lorsque l'antivirus utilisé ne contient pas de fonction de détection des logiciels indésirables (Malware), le compléter par une application effectuant ces fonctions (Malwarebytes est l'un des plus connus et efficaces disponible en version gratuite). Mettre à jour régulièrement ses logiciels, système d'exploitation et applications (les extensions des navigateurs, Flash Player par exemple, sont d'importants vecteurs d'infection).

Extensions classiques des fichiers cryptés : .ecc, .ezz, .exx, .zzz, .xyz, .aaa, .abc, .ccc, .vvv, .xxx, .ttt, .micro, .encrypted, .locked, .crypto, _crypt, .crinf, .r5a, .XRNT, .XTBL, .crypt, .R16M01D05, .pzdc, .good, .LOL!, .OMG!, .RDM, .mp3, .RRK, .encryptedRSA, .crjoker, .EnCiPhErEd, .LeChiffre, .keybtc@inbox_com, .0x0, .bleep, .1999, .vault, .HA3, .toxcrypt, .magic, .SUPERCRYPT, .CTBL, .CTB2, .locky

Fichiers de notes laissés dans un répertoire ayant été crypté : HELP*DECRYPT.TXT, HELP_YOUR_FILES.TXT, HELP_TO_DECRYPT_YOUR_FILES.txt, RECOVERY_KEY.txt HELP_RESTORE_FILES.txt, HELP_RECOVER_FILES.txt, HELP_TO_SAVE_FILES.txt, DecryptAllFiles.txt DECRYPT_INSTRUCTIONS.TXT, INSTRUCCIONES_DESCIFRADO.TXT, How_To_Recover_Files.txt YOUR_FILES.HTML, YOUR_FILES.url, encryptor_raas_readme_liesmich.txt, Help_Decrypt.txt DECRYPT_INSTRUCTION.TXT, HOW_TO_DECRYPT_FILES.TXT, ReadDecryptFilesHere.txt, Coin.Locker.txt _secret_code.txt, About_Files.txt, Read.txt, ReadMe.txt, DECRYPT_ReadMe.TXT, DecryptAllFiles*.txt FILESAREGONE.TXT, IAMREADYTOPAY.TXT, HELLOTHERE.TXT, READTHISNOW!!!.TXT, SECRETIDHERE.KEY IHAVEYOURSECRET.KEY, SECRET.KEY, HELP*DECYPRT_YOUR_FILES.HTML, help_decrypt_your_files.html HELP_TO_SAVE_FILES.txt, RECOVERY_FILES.txt, RECOVERY_FILE.TXT, RECOVERY_FILE*[random].txt Howto*RESTORE_FILES*.txt, Howto*Restore_FILES.txt, howto_recover_file*.txt, restore*files*.txt, how*recover+[random].txt, _how_recover*.txt, recovery*file*[random].txt, recover*file*[random].txt recovery*file*[random].txt, Howto_Restore_FILES.TXT, help_recover_instructions+[random].txt, _Locky_recover_instructions.txt

** le texte [random] signifie une suite aléatoire de lettres et chiffres inclus dans le nom du fichier.

Ces fichiers contiennent les instructions de paiement et de récupération de la clé. À noter que le paiement de la rançon ne garantit pas la récupération de la clé : celle-ci dépend de « l'honnêteté » des pirates!