SIMPLY SECURE

G DATA WHITEPAPER

RANSOMWARE : APERÇU DES MENACES ET SOLUTIONS

Sommaire

Définition du ransomware **2**

Les techniques d'attaque **2**

Les vulnérabilités logicielles en ligne de mire **2**

Les bloquer, possible ? **3**

Les mesures pour limiter les risques **3**

Les solutions après infection **5**

À propos des solutions G DATA **5**

Définition du ransomware

Le Ransomware (ou rançongiciel) est un type d'attaque visant à demander une rançon à la victime. Dans sa forme électronique, l'objet général de l'attaque est l'accès aux données de l'utilisateur ou à son système d'exploitation. Il existe deux principaux types de ransomware : les screen lockers et les crypto trojans. Les premiers bloquent le système dès le démarrage, mais ne demandent pas à proprement parler une rançon. Ces attaques usurpent l'identité d'instances judiciaires et avancent des manquements à la loi. Téléchargements illégaux, visites de sites pédopornographiques, etc. sont avancés afin de faire payer une « amende » à l'utilisateur. Le représentant le plus connu de ce type de ransomware est le "FBI Trojan ", aussi connu sous le nom de Reveton. Les crypto lockers ciblent quant à eux les données de la victime. Photos, documents, feuilles de calcul, bases de données et tout autre fichier de l'utilisateur sont ciblés. Contrairement aux screen lockers, les crypto lockers ne camouflent pas leurs actions. Une fois le code malveillant dans le système, ils chiffrent de manière forte les données et demandent à la victime de payer une rançon. Les paiements doivent alors être réalisés en Bitcoin ou toute autre monnaie virtuelle. En théorie, le paiement de la rançon permet à la victime de récupérer la clé de déchiffrement pour récupérer ses fichiers. Mais en pratique, rien n'assure que l'attaquant tiendra ses promesses… Il existe des centaines variantes de ransomware tels que cryptolocker, CryptoWall, VaultCrypt ou encore CTB-Locker. Beaucoup plus nuisibles et plus puissants que les screen lockers, les crypto lockers sont actuellement les ransomwares les plus répandus.

Les techniques d'attaque

Une des techniques les plus fréquemment utilisées pour diffuser un ransomware est ce qu'on appelle l'ingénierie sociale ("social engineering" en anglais).
Cette technique exploite les différents comportements humains pour infecter les systèmes. Un cas classique est un courrier électronique qui semble être une confirmation de commande. Ces courriers contiennent une pièce jointe que la victime est invitée à ouvrir. Si la victime reçoit un email lui confirmant une commande, il y a beaucoup de chances qu'elle ouvre la pièce jointe. Dans le cas où elle a justement réalisé une commande quelques minutes plus tôt, elle sera en confiance et ouvrira la pièce jointe. Si elle n'a pas fait de commande, il y a une forte probabilité qu'elle ouvre la pièce jointe afin d'obtenir plus d'informations sur celle-ci.

L'approche par ingénierie sociale n'est pas la seule méthode d'attaque. Chaque internaute peut également tomber sur un ransomware en naviguant sur Internet. Il suffit pour cela que le site visité ait été compromis pour diffuser des malwares. Avec cette technique d'attaque, dite « drive by », il n'est pas nécessaire de cliquer ou de lancer de façon active un téléchargement : le code malveillant est injecté directement dans le système. Pour cela, les attaquants intègrent des exploits kits dans des sites Internet vulnérables (non mis à jour par le webmaster ou protégés par des mots de passe faibles) qui diffusent alors leur malware aux visiteurs mal protégés. Le simple affichage de la page ou d'une bannière suffit.

Les vulnérabilités logicielles en ligne de mire

Comme beaucoup de logiciels malveillants, le ransomware utilise des vulnérabilités logicielles pour attaquer le système. Ces vulnérabilités sont présentes dans des logiciels non régulièrement mis à jour par l'utilisateur. Les logiciels les plus répandus, tels que Microsoft Office, Adobe Acrobat Reader, Java ou Windows lui-même, sont les plus utilisés par les attaquants. L'exploitation de ces vulnérabilités se réalise par des exploits kit. Une fois chargés dans la mémoire du système, ces exploits téléchargent le reste du code sur des serveurs distants et l'exécutent.

Pendant ce temps, le composant installé contacte le « centre de commande », génère la clé de chiffrement et commence à chiffrer les fichiers. Une fois que le message de rançon est affiché, il est généralement trop tard pour arrêter le chiffrement des fichiers.

Les bloquer, possible ?

Les ransomware sont devenus problématiques durant ces derniers mois, voire ces dernières années. L'année 2013 a connu l'arrivée du "Cryptolocker" qui a engendré beaucoup de variantes depuis. Cela n'est pas passé inaperçu pour les fabricants d'antivirus qui ont dû redoubler d'efforts pour endiguer le nombre croissant de ransomware. L'arsenal antivirus contient beaucoup d'armes, mais aucune d'elles ne peut empêcher complètement une infection par ransomware. La détection classique basée sur les signatures reste la colonne vertébrale de la défense AV, mais elle n'est plus suffisante. Pour toute pièce jointe d'email détectée par une signature, un nombre important de pièces jointes ne sont pas détectées. Davantage de mécanismes proactifs sont donc nécessaires, tels que les analyses comportementales, capables de détecter les activités anormales du système. D'autres protections dites « 0-day » sont également requises. Celles-ci doivent être capables de bloquer des exploitations de failles et des attaques sans nécessiter de mises à jour. Le développement de ces modules de protection autonomes et proactives constitue une priorité pour les chercheurs G DATA.
Pourquoi n'y a-t-il pas de solution anti-ransomware dédiée ? Si techniquement, mettre en place une solution anti-ransomware qui assurerait un blocage quasi total est possible, le problème se situerait au niveau des performances système et du confort utilisateur. Analyser chaque processus et augmenter le niveau de détection comportementale au maximum engendreraient lenteurs et blocages intempestifs du système et des programmes. Le challenge est de minimiser l'empreinte sur la performance et de maximiser l'efficacité.

Les mesures pour limiter les risques

Sauvegardes

Car toute donnée chiffrée par un ransomware n'est plus accessible, l'une des principales démarches est de sauvegarder régulièrement ces données. La sauvegarde doit être réalisée quotidiennement et, dans l'idéal, déconnectée ensuite du système. Il est par exemple déconseillé d'opter pour l'utilisation de lecteurs réseau sans droits d'utilisation spécifiques (mot de passe, quota, droit en lecture/écriture). Ces espaces étant également visés par les ransomwares, leur chiffrement peut conduire au blocage de tout ou une partie de l'espace de stockage partagé d'une entreprise.

Mises à jour

La seconde mesure de sécurité est de maintenir les logiciels et le système d'exploitation à jour. Les logiciels malveillants en général infectent très souvent les systèmes en exploitant les vulnérabilités non corrigées. Dans un réseau d'entreprise, s'assurer que les ordinateurs clients sont à jour et procéder aux corrections si besoin est un processus fastidieux. Mais des solutions pour les entreprises sont là pour faciliter la tâche. C'est par exemple le cas de G DATA PatchManagement qui permet de réaliser audit et déploiement des correctifs de manière centralisée.

Stratégies de groupe

Dans un environnement professionnel, mettre en place certaines règles de groupes dans Active Directory peut également aider à minimiser la surface d'attaque. Une de ces solutions, bien que très restrictives, consiste à bloquer toutes les applications qui ne sont pas exécutées à partir d'un des dossiers "Program Files". Cette règle se

réalise en utilisant la "Politique de restriction logicielle" (Software Restriction Policy). Pour cela, une nouvelle politique de groupe doit être créée dans gpmc.msc.
L'option correspondante est localisée sous Configuration ordinateur/Paramètres Windows/Paramètres de sécurité/Stratégies de restriction logicielle/Niveaux de sécurité. Aucune restriction n'est activée par défaut. En l'activant, seuls les programmes installés dans C:\Program Files (x86) peuvent être exécutés. Sous « Règles additionnelles », des exceptions peuvent être créées.

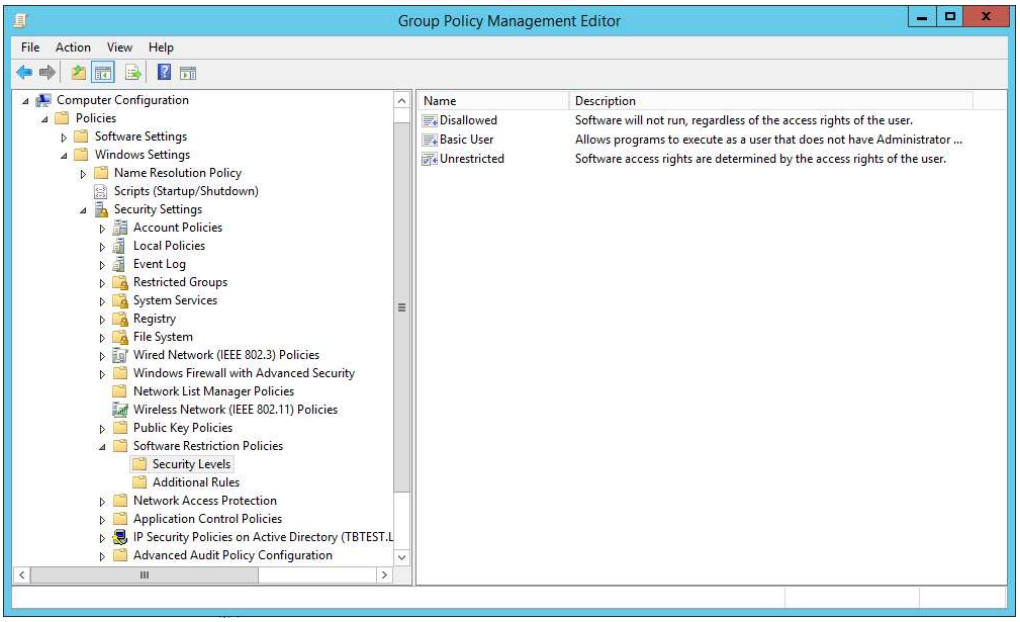

Figure 1: Stratégies de restriction logicielles

Gestion de droits

Restreindre les droits d'écriture dans les partages réseau est un réglage qui doit être envisagé. La manipulation des pièces jointes d'email doit également être maîtrisée. L'utilisation de fichiers exécutables (.exe) ou compressés (.zip) étant limitée à des utilisations professionnelles spécifiques, elle doit être bloquée pour tous les utilisateurs ou services n'en ayant pas l'utilité. Ces restrictions peuvent être réalisées à partir de passerelles de messagerie antispam et antivirus, comme celle de G DATA MailSecurity.

Pour aller plus loin dans la gestion des droits et ainsi réduire la surface d'attaque, des outils centralisés de gestion de stratégies peuvent être utilisés. Ceux-ci apportent un niveau de réglage pointu, le tout centralisé dans une console de gestion centralisée. C'est par exemple ce que permet la solution G DATA ENPOINT PROTECTION.

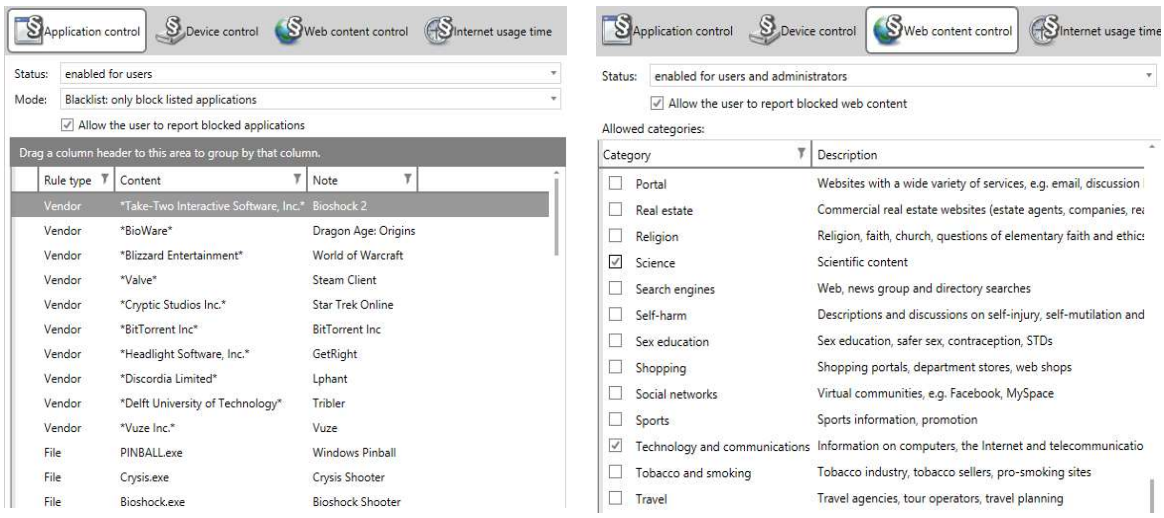

Figure 4 : contrôle des programmes et d'Internet dans le G DATA PolicyManager

Les solutions après infection

Un ou plusieurs clients de votre réseau ont été infectés ? Voici ci-dessous quelques conseils à appliquer :

a) Ne payez pas la rançon demandée. Tout d'abord parce que le paiement ne garantit pas la restitution des données. Ensuite parce que procéder au paiement, c'est financer les réseaux cybercriminels et le crime organisé.

b) Déconnectez immédiatement du réseau le système infecté, cela afin d'éviter la propagation du malware sur d'autres clients ou sur des partages réseau.

c) Le système infecté doit être considéré comme dangereux. Autrement dit, tout support de stockage qui y était connecté lors de l'attaque, ou qui y serait connecté ensuite, ne doit pas être connecté dans le réseau ou sur un autre ordinateur sans formatage préalable.

d) Si la typologie du ransomware ne permet pas de récupérer les données, sa restauration à partir d'une sauvegarde sera nécessaire.

e) Si le système a été touché par un screen locker, il est possible de trouver des instructions sur Internet afin de débloquer le système.

À propos des solutions G DATA

Les logiciels de sécurité de l'éditeur allemand couvrent tous les besoins de protection contre les malwares et les attaques auxquels peuvent être confrontés entreprises et utilisateurs particuliers. Pour lutter efficacement contre les ransomware, G DATA intègre plusieurs outils de protection dans ses solutions, avec notamment la technologie Exploit Protection. Elle bloque l'exploitation des failles de sécurité présentes dans les logiciels non mis à jour. Des modules complémentaires tels que PatchManagement, MailSecurity ou PolicyManagement, peuvent également aider à lutter contre les attaques par ransomware.

Pour en savoir plus sur les solutions G DATA : www.gdata.fr