KASPERSKY lab

Sauvegarde des données de l'utilisateur avec Kaspersky Cryptomalware Countermeasures Subsystem

Les cybercriminels sont prompts à adopter les techniques développées par les criminels dans le monde réel, y compris en extorquant de l'argent à leurs victimes. Dans l'un des scénarios d'attaque ransomware les plus courants, le cybercriminel consulte les données chiffrées de l'utilisateur avant d'exiger de l'argent. Les utilisateurs accordant une grande valeur à leurs données, ils sont nombreux à accepter de payer pour préserver leurs précieux fichiers. Pourtant, payer n'est pas une sage décision, principalement parce qu'il n'y a aucune garantie que les données corrompues ne seront pas déchiffrées. Dans le même temps, un cryptomalware moderne utilise des schémas de chiffrement qui (jusqu'à présent) semblent être inviolables si bien que les victimes ont le choix entre payer ou perdre leurs fichiers. Bien sûr, si un logiciel de sécurité Internet fiable est installé sur l'ordinateur, il réagira aux activités malveillantes. Cependant, même les meilleures solutions de protection contre les programmes malveillants ne peuvent détecter avec succès les derniers cryptomalwares developpés qu'une fois qu'ils ont commencé à corrompre les données. En conséquence, un programme malveillant jusque-là invisible et qui n'apparaît pas dans la base de données parvient de temps en temps à chiffrer quelques fichiers avant d'être neutralisé. C'est pourquoi Kaspersky Lab a développé son sous-système Cryptomalware Countermeasures Subsystem.

Menace de type cryptomalware

Un cryptomalware est généralement distribué à l'aide de messages indésirables auxquels sont joints des fichiers exécutables qui ressemblent à des documents, mais il peut également se propager par d'autres moyens. Par exemple, il existe des cas d'installations de cryptomalwares par un autre programme malveillant (un cheval de Troie de la famille Zeus/Zbot) ont été signalés.

La menace de type cryptomalware ne cesse d'augmenter. Le programme Kaspersky Security Network montre qu'en 2013, quelque 2,8 millions de crypto-attaques ont été enregistrées, soit neuf fois plus qu'en 2012, et tous les éléments de preuve indiquent que ce nombre continuera d'augmenter car de nombreuses personnes sont encore disposées à payer la rançon demandée. Selon une enquête réalisée par le centre de recherche interdisciplinaire de cyber-sécurité à l'Université de Kent, en février 2014, plus de 40 % des victimes de Cryptolocker ont accepté de payer. En outre, le rapport de Dell SecureWorks montre que ces mêmes programmes malveillants permettent d'engranger jusqu'à 30 millions de dollars tous les 100 jours.

De plus, l'incapacité à décrypter les fichiers chiffrés par les programmes malveillants modernes engendre une menace supplémentaire - un faux remède. Les utilisateurs désespérés par la perte de leurs fichiers recherchent de l'aide sur Internet et trouvent parfois un programme prétendument conçu pour « déchiffrer » les données chiffrées. Dans le meilleur des cas, ce n'est qu'une escroquerie qui propose une « solution » inutile, dans le pire des cas, ce programme propage d'autres programmes malveillants.

Évolution des programmes malveillants de chiffrement

Les méthodes criminelles deviennent de plus en plus sophistiquées d'année en année. Le premier cryptomalware utilisait un algorithme reposant sur une clé symétrique, la même clé étant utilisée pour le chiffrement et le déchiffrement. Généralement, grâce à l'aide de quelques éditeurs de solutions de protection contre les programmes malveillants, il était possible de déchiffrer les informations corrompues. Puis, les cybercriminels ont commencé à mettre en œuvre des algorithmes de cryptographie à clé publique utilisant deux clés distinctes : une clé publique pour chiffrer les fichiers et une clé privée pour les déchiffrer. L'un des premiers cryptosystèmes utilisant des clés publiques que les cybercriminels ont utilisé s'appelait RSA (pour Ron Rivest, Adi Shamir et Leonard Adleman, les premiers à avoir décrit cet algorithme). En 2008, les experts de Kaspersky Lab ont réussi à craquer une clé RSA de 660 bits utilisée par le cheval de Troie GPCode. Cependant, les créateurs de ce code n'ont pas tardé à mettre la clé à niveau en la passant à 1024 bits, rendant ainsi le déchiffrement encore plus difficile.

L'un des programmes les plus récents et dangereux de cryptomalware, le cheval de Troie Cryptolocker précédemment mentionné, utilise également un algorithme basé sur une clé publique. Après avoir infecté un ordinateur, il se connecte au serveur de commande et de contrôle pour télécharger la clé publique de sorte que l'autre clé (la clé privée) n'est accessible que par les créateurs de Cryptolocker. La victime n'a généralement pas plus de 72 heures pour payer la rançon avant que la clé privée ne soit définitivement supprimée. Le déchiffrement des fichiers est impossible sans cette clé. Les produits Kaspersky Lab détectent ce cheval de Troie, mais si le système est déjà infecté, les fichiers corrompus sont définitivement perdus.

Figure 1. Écran de demande de rançon de Cryptolocker

Cryptomalware Countermeasures Subsystem de Kaspersky Lab

A l'heure actuelle, il est impossible de déchiffrer les fichiers chiffrés avec un cryptomalware moderne. La seule contre-mesure efficace pour les utilisateurs consiste à conserver une copie de sauvegarde de leurs fichiers. Cependant, une sauvegarde générale, même régulière, n'offre pas une protection suffisante puisque les fichiers récemment modifiés ne sont pas protégés. C'est pourquoi Kaspersky Lab a développé une autre contre-mesure, reposant sur le module System Watcher.

Kaspersky System Watcher analyse les données d'événements les plus pertinentes du système, y compris les informations relatives à la modification des fichiers. Lorsqu'il détecte qu'une application suspecte tente d'ouvrir les fichiers personnels d'un utilisateur, il effectue immédiatement une copie de sauvegarde locale protégée de ces derniers[1]. S'il s'avère par la suite que l'application est malveillante, Kaspersky System Watcher annule automatiquement les modifications non sollicitées. Par conséquent, l'utilisateur n'a pas besoin de faire quoi que ce soit à l'encontre des cryptomalwares. Il sera simplement notifié de la mise à jour de la progression du processus de protection.

[1] *Chaque fichier sauvegardé ne doit pas dépasser 10 Mo.*

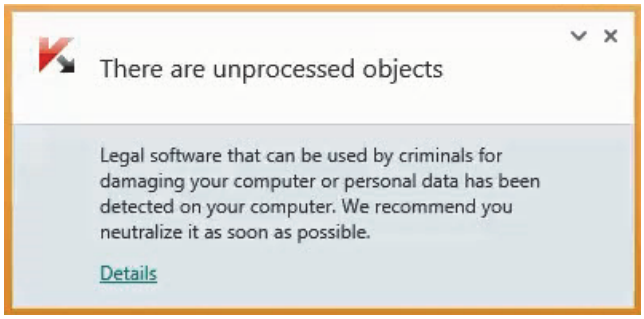

Figure 2. System Watcher constate qu'une application modifie des fichiers de façon suspecte et avertit l'utilisateur. À ce moment, il crée des copies de sauvegarde protégées des fichiers et analyse la nature des modifications apportées

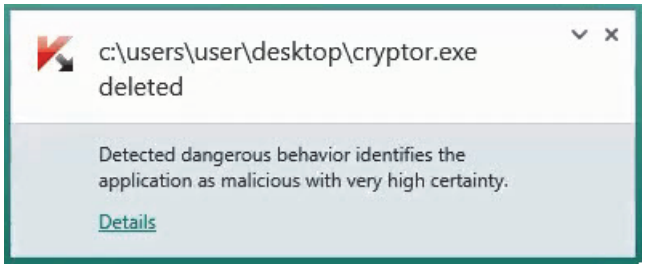

Figure 3. L'application est bien un programme malveillant. Le fichier qui contient le programme malveillant est supprimé. Les fichiers affectés restent chiffrés

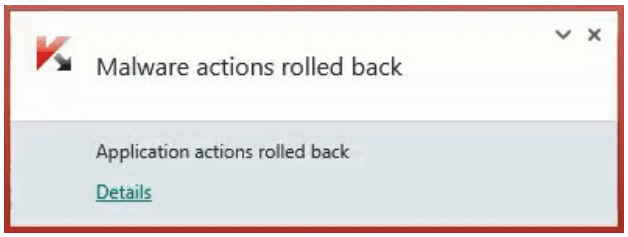

Figure 4. System Watcher remplace les fichiers chiffrés par les copies de sauvegarde. Une fois toutes les conséquences du cryptomalware supprimées, System Watcher signale que toutes les actions malveillantes ont été annulées

Par conséquent, même si un nouveau cryptomalware utilise une vulnérabilité « zero-day » en veillant à éviter tous les systèmes de sécurité, il ne provoquera pas de dommage, car toutes les modifications seront automatiquement annulées. En d'autres termes, Cryptomalware Countermeasures Subsystem protège les données de l'utilisateur et interrompt le financement des cybercriminels. En effet, payer la rançon demandée ne fera que les encourager à poursuivre leurs actions en créant rapidement davantage de programmes malveillants.

Disponibilité

Le sous-système Cryptomalware Countermeasures Subsystem est intégré au composant System Watcher, lui-même intégré aux produits destinés aux particuliers et aux entreprises suivants :

Pour les particuliers

- Kaspersky Internet Security
- Kaspersky Internet Security – Multi-Device (pour Windows uniquement)
- Kaspersky PURE
- Kaspersky Anti-Virus

Pour les entreprises

- Kaspersky Endpoint Security for Business
- Kaspersky Small Office Security