Dossier technique

Comment se protéger des logiciels de demande de rançon

Contrez le ransomware grâce aux solutions Intel® Security

Les logiciels de demande de rançon (ransomware) sont des logiciels malveillants qui ont recours au chiffrement asymétrique pour prendre en otage les données d'une victime. Le chiffrement asymétrique (public-privé) est une technique cryptographique utilisant une paire de clés numériques pour chiffrer et déchiffrer un fichier. La paire de clés publique-privée est générée de façon unique par le pirate à l'intention de la victime, la clé privée servant à déchiffrer les fichiers stockés sur le serveur du pirate. Après paiement de la rançon, ce dernier communique la clé privée à la victime — du moins en théorie, car ce n'est pas toujours le cas, comme nous avons pu le constater lors de récentes campagnes de ransomware. Sans accès à la clé privée, il est pratiquement impossible de déchiffrer les fichiers pris en otage.

Il existe de nombreuses variantes des logiciels de demande de rançon en circulation. Souvent, les ransomwares (et autres logiciels malveillants) sont distribués dans le cadre de campagnes de spam, et parfois par le biais d'attaques ciblées. Les produits Intel® Security mettent en œuvre une série de technologies permettant de bloquer les logiciels de demande de rançon. Les produits McAfee® et configurations associées suivants sont conçus pour bloquer de nombreux types de ransomwares.

McAfee VirusScan® Enterprise 8.8 ou McAfee Endpoint Security 10

- Maintenez les fichiers DAT à jour.
- Assurez-vous que McAfee Global Threat Intelligence (McAfee GTI) est activé, car ce système contient plus de 8 millions de signatures de ransomwares uniques.
- Mettez au point des règles de protection de l'accès pour bloquer l'installation des charges actives de ransomware. Reportez-vous aux articles de la base de connaissances consacrés aux règles de protection de l'accès : KB81095 et KB54812.

McAfee Host Intrusion Prevention

- Visionnez une vidéo expliquant comment configurer McAfee Host Intrusion Prevention pour bloquer la charge active de CryptoLocker.
- Activez la signature 3894 de Host Intrusion Prevention, Access Protection—Prevent svchost.exe executing non-Windows executables (Protection à l'accès - Empêcher le lancement de fichiers exécutables non-Windows par svchost).
- Activez les signatures 6010 et 6011 de Host Intrusion Prevention pour bloquer immédiatement les injections.

intel Security

Règles McAfee Host Intrusion Prevention
McAfee Host Intrusion Prevention prend en charge la surveillance des opérations de création, lecture, écriture, exécution, suppression, modification du nom et modification d'attribut des fichiers, ainsi que de création de liens physiques. Définissez les chemins/types de fichiers pour lesquels vous souhaitez recevoir des alertes, et les exécutables que vous souhaitez inclure (sources malveillantes connues) ou exclure (générateurs de faux positifs connus). Dans la mesure où cette règle peut potentiellement être intrusive, il est recommandé de l'utiliser en mode informatif/de journalisation pendant une période d'évaluation. Notez que les règles de protection des fichiers nécessitent la mise en œuvre d'une base de données d'applications approuvées.

Rule: Cryptolocker—block EXE in AppData

Rule type: files

Operations: create, execute, write

Parameters:
- Include: Files: **\AppData*.exe
- Include: Files: **\AppData\Local*.exe
- Include: Files: **\AppData\Roaming*.exe

Executables: Include *.*

L'exemple suivant omet de nombreuses extensions de fichier pour des questions de contraintes d'espace. Veillez à sélectionner toutes les extensions de fichier applicables pour vos applications.

Rule {

tag “Blocking a Non-Trusted program attempt to write to protected data file extensions”

Class Files

Id 4001

level 4

files {Include “**.3DS” “**.7Z” “**.AB4” “**.AC2” “**.ACCDB” “**.ACCDE” “**.ACCDR” “***.ACCDT” “**.ACR” “**.ADB” “**.AI” “**.AIT” “**.al” “**.APJ” “**.ARW” “**.ASM” “**.ASP” “**.BACKUP” “**.BAK” “**.BDB” “**.BGT” “**.BIK” “**.BKP” “**.BLEND” “**.BPW” “**.C” “**.CDF” “**. CDR” “**.CDX” “**.CE1” “**.CE2” “**.CER” “**.CFP” “**.SRF” “**.SRW” “**.ST4” “**.ST5” “**.ST6” “**.ST7” “**.ST8” “**.STC” “**.STD” “**. STI” “**.STW” “**.STX” “**.SXC” “**.SXD” “**.SXG” “**.SXI” “**.SXM” “**.SXW” “**.TXT” “**.WB2” “**.X3F” “**.XLA” “**.XLAM” “**.XLL” “**. XLM” “**.XLS” “**.XLSB” “**.XLSM” “**.XLSX” “**.XLT” “**.XLTM” “**. XLTX” “**.XLW” “**.XML” “**.ZIP”}

Executable {Include “*”}

user_name{Include “*”}

directives files:writefiles:renamefiles:delete

}

- Règles de protection de l'accès : Vous pouvez également utiliser les règles de protection de l'accès pour renforcer la règle Host Intrusion Prevention grâce à l'utilisation des caractères génériques : **\Users**\AppData***.exe

Remarque : avec les nouvelles versions de SYSCore fournies par les versions mises à jour de McAfee VirusScan Enterprise, McAfee Agent, Host Intrusion Prevention et Data Loss Prevention, les caractères « ** » ne fonctionnent plus au début du champ « File or folder name to block » (Nom du fichier ou du dossier à bloquer). Avec les nouvelles versions, vous devez utiliser le format suivant :

```
C:\**\AppData\**.exe
```

Cette règle est conçue pour bloquer tout fichier .exe à la racine et tout sous-répertoire d'un dossier nommé AppData situé n'importe où sur le lecteur C.

Les itérations possibles d'une règle de ce type sont pratiquement illimitées. Il est donc recommandé d'envisager soigneusement tous les aspects de la règle. Il faut prendre en considération tous les aspects de la règle et toutes les entrées possibles pour sa fonction prévue, et savoir comment configurer les règles en général (exemple ci-dessous) :

Process to include: *

Process to exclude: [laisser vide]

File or folder name to block: <chemin ou répertoire>

File actions to prevent: [Toutes les actions souhaitées — Il est recommandé de commencer par les actions moins agressives pour limiter au maximum les perturbations possibles au niveau des terminaux.]

McAfee SiteAdvisor® Enterprise ou Endpoint Security/Web Protection

- Utilisez les informations sur la réputation des sites web pour avertir les utilisateurs de la présence de logiciels de demande de rançon sur les sites visités ou bloquer l'accès à ces sites.

McAfee Threat Intelligence Exchange avec Advanced Threat Defense

- Configuration des stratégies Threat Intelligence Exchange :
  - Commencez en mode d'observation. Lorsque des processus suspects sont identifiés sur des terminaux, utilisez les marqueurs système pour appliquer les stratégies de mise en œuvre de Threat Intelligence Exchange.
  - Nettoyez au niveau « Known malicious » (Malveillant connu).
  - Bloquez au niveau « Most-likely malicious » (Très probablement malveillant). (Un blocage au niveau « Unknown » (Inconnu) offrirait une meilleure protection mais peut également alourdir la charge administrative initiale.)
  - Configurez l'option « Submit files to McAfee Advanced Threat Defense » (Envoyer les fichiers à McAfee Advanced Threat Defense) aux niveaux « Unknown » (Inconnu) et inférieurs.
  - Stratégie Threat Intelligence Exchange Server : Acceptez les réputations Advanced Threat Defense pour les fichiers qui n'ont jamais été rencontrés par McAfee Threat Intelligence Exchange.
- Intervention manuelle dans Threat Intelligence Exchange :
  - Mise en œuvre de la réputation des fichiers (suivant le mode de fonctionnement) : « Most likely malicious » (Très probablement malveillant) ; choisissez de nettoyer/supprimer.
  - « Might be malicious » (Potentiellement malveillant) : bloquer.
- La réputation d'entreprise (organisationnelle) peut outrepasser McAfee GTI :
  - Vous pouvez choisir de bloquer un processus indésirable, par exemple une application non prise en charge ou vulnérable.
  - Marquez le fichier comme « Might be malicious » (Potentiellement malveillant).

- Vous pouvez également choisir d'autoriser un processus indésirable à des fins de test.
  - Marquez le fichier comme « Might be trusted » (Potentiellement approuvé).

McAfee Advanced Threat Protection

- Fonctionnalités de détection prédéfinies :
  - Détection basée sur les signatures : McAfee Labs dispose actuellement de plus de 8 millions de signatures de ransomware, notamment pour CTB-Locker, CryptoWall et leurs variantes.
  - Détection basée sur la réputation : McAfee GTI.
  - Émulation et analyse statique en temps réel : Utilisées pour la détection sans signatures.
  - Règles YARA personnalisées.
  - Analyse de code statique complète : Cette analyse reconstitue la logique du code pour évaluer l'état des attributs et des jeux de fonctions, et effectuer un examen approfondi du code source sans l'exécuter.
  - Analyse dynamique dans un environnement restreint de type sandbox.
- Créez des profils d'analyse sur les systèmes et programmes susceptibles d'être ciblés par les logiciels de demande de rançon :
  - Systèmes d'exploitation courants, Windows 7, Windows 8, Windows XP
  - Applications Windows installées (Word, Excel) avec macros activées
- Autorisez les profils d'analyse à accéder à Internet :
  - De nombreux échantillons exécutent un script à partir d'un document Microsoft, qui établit une connexion sortante et active le logiciel malveillant. Autoriser les profils d'analyse à accéder à Internet permet d'améliorer les taux de détection.

McAfee Network Security Platform

- Les stratégies par défaut de Network Security Platform contiennent des signatures permettant de détecter les logiciels malveillants :
  - Vérifiez que vous disposez de la signature id=0x4880f900 (propre aux logiciels de demande de rançon).
  - Network Security Platform comporte également des signatures permettant d'identifier Tor, qui peut être utilisé pour transférer des fichiers associés aux logiciels malveillants.
- Intégration avec Advanced Threat Defense pour les nouvelles variantes des attaques :
  - Configurez l'intégration avec Advanced Threat Defense dans la stratégie pour les logiciels malveillants avancés.
  - Configurez Network Security Platform pour envoyer les fichiers .exe, Microsoft Office, Java Archive et PDF à Advanced Threat Protection pour inspection.
  - Vérifiez que la configuration d'Advanced Threat Protection est appliquée au niveau des capteurs.
- Mettez à jour les règles de détection des rappels (réseaux de robots).

McAfee Web Gateway

- Activez l'inspection McAfee Gateway Anti-Malware.
- Activez McAfee GTI pour tirer parti du service de réputation des fichiers et des URL.
- Intégrez la solution avec McAfee Advanced Threat Defense pour bénéficier de fonctions sandbox et de détection des menaces de type « jour zéro ».

VirusTotal Convicter : intervention automatisée

- Convicter est un script Python déclenché par le système de réponse automatisée de McAfee ePolicy Orchestrator® (McAfee ePO™) pour référencer un fichier générant un événement de menace McAfee Threat Intelligence Exchange avec VirusTotal.

- Notez que vous pouvez modifier le script pour recouper les événements avec d'autres modules Threat Intelligence Exchange, tels que GetSusp.
- Si le seuil de confiance dans la communauté est atteint, le script définit automatiquement la réputation de l'entreprise.
- Seuil d'identification positive suggéré : 30 % des éditeurs, dont deux éditeurs majeurs, doivent confirmer.
- Filtre : Target File Name Does Not Contain (Le nom du fichier cible ne contient pas) : McAfeeTestSample.exe.
- GetSusp est un outil gratuit dont le support est assuré par la communauté. (Le support n'est pas pris en charge par McAfee/Intel Security.)

McAfee Active Response
Active Response détecte et neutralise les menaces avancées. Lorsqu'il est utilisé en association avec des flux d'informations sur les menaces tels que McAfee GTI, Dell SecureWorks ou ThreatConnect, les nouvelles menaces (dont les ransomwares) peuvent être recherchées et éliminées avant qu'elles n'aient l'occasion de se propager.

- Les collecteurs personnalisés vous permettent de créer des outils spécifiques afin de rechercher et d'identifier les indicateurs de compromission associés aux logiciels de demande de rançon.
- L'utilisateur intègre des déclencheurs et des réactions pour définir les actions exécutées lorsque des conditions spécifiques sont remplies. Par exemple, lorsque des hachages ou des noms de fichiers sont détectés, une action de suppression peut être automatiquement exécutée.

Autres lectures conseillées

Protecting Against Ransomware (Protection contre les logiciels de demande de rançon)
Cet article de la base de connaissances propose aux clients des informations détaillées récentes pour se protéger contre les logiciels de demande de rançon dans un environnement Intel Security.

Pour tout savoir des différentes variantes du ransomware CryptoLocker, des symptômes, des vecteurs d'attaque et des techniques de prévention, regardez les vidéos suivantes :

- CrytpoLocker Malware Session (Présentation du logiciel malveillant CrytpoLocker)
- CryptoLocker Update (Dernières infos sur CryptoLocker)

Avis sur les menaces McAfee Labs : X97M/Downloader
Cet article propose une analyse détaillée d'une des dernières versions du logiciel de demande de rançon.

Échec et mat aux logiciels de demande de rançon : ne laissez pas vos données se faire prendre en otage
Cette présentation de solution de cinq pages explique ce que sont les logiciels de demande de rançon et comment certaines solutions Intel Security (mais pas toutes) permettent de s'en protéger.

Advice for Unfastening CryptoLocker Ransomware (Conseils pratiques pour contrer le logiciel de demande de rançon CryptoLocker)
Billet de blog décrivant en détail ce qu'un client doit faire s'il est victime d'une attaque de logiciel de demande de rançon.

Le retour du ransomware : de nouvelles familles arrivent en force
Article du Rapport de McAfee Labs sur le paysage des menaces (p. 14) décrivant les nouveaux logiciels de demande de rançon et les variantes.

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com