Présentation de solution

Protéger les systèmes de soins de santé contre les logiciels de demande de rançon

Les logiciels de demande de rançon (ransomware) sont des logiciels malveillants qui recourent généralement au chiffrement asymétrique pour prendre en otage les données d'une victime. Le chiffrement asymétrique (public-privé) est une technique cryptographique qui utilise une paire de clés pour chiffrer et déchiffrer un fichier. La paire de clés publique et 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 — même si 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.

Ces dernières années, le ransomware est devenu un sujet préoccupant pour tous les professionnels de la sécurité. Malheureusement, il s'agit d'un outil de cyberattaque simple, efficace et très lucratif. Au cours de l'année écoulée, le choix des cibles a évolué : ce sont désormais les entreprises, et plus les particuliers, qui en sont victimes car elles ont les moyens de payer des rançons plus élevées. Voici peu, ce sont les hôpitaux qui sont devenus des cibles de prédilection de certains auteurs de logiciels de demande de rançon. Le *Rapport de McAfee Labs sur le paysage des menaces — Septembre 2016* propose une analyse des attaques de ransomware lancées aux 1er et 2e trimestres 2016 contre des hôpitaux et explique les raisons du succès de ces attaques ciblées et liées, en dépit de leur relative simplicité. Il se penche aussi sur la problématique du ransomware dans le milieu hospitalier, notamment les défis posés par des anciens systèmes et des équipements médicaux mal sécurisés, ainsi que l'importance vitale de l'accès instantané à l'information.

intel Security

Stratégies et procédures de protection contre le ransomware

Pour protéger les systèmes contre les logiciels de demande de rançon, il est essentiel d'être conscient du problème et informé des modes de propagation de ces menaces. Voici plusieurs stratégies et procédures que les hôpitaux devraient mettre en œuvre pour limiter les chances de succès d'une attaque de ransomware :

- Élaborez un plan d'action qui pourra être mis à exécution dans l'éventualité d'une attaque. Sachez où résident les données critiques et déterminez s'il existe un moyen de les infiltrer. Effectuez des exercices de reprise après sinistre et de continuité des activités avec la cellule d'urgence de l'hôpital, pour valider les objectifs de délai et de point de reprise. Ces exercices peuvent permettre d'identifier des conséquences cachées sur le fonctionnement de l'hôpital qui n'apparaissent pas lors des tests de sauvegarde habituels. La plupart des hôpitaux ont dû verser la rançon car ils ne possédaient pas de plan de secours.
- Veillez à appliquer les correctifs nécessaires aux systèmes. De nombreuses vulnérabilités exploitées par les logiciels de demande de rançon peuvent être corrigées. Installez les derniers correctifs disponibles pour les systèmes d'exploitation, Java, Adobe Reader, Flash et les différentes applications. Mettez en place une procédure de déploiement des patchs et correctifs, et vérifiez si ceux-ci ont été correctement appliqués.
- Pour les systèmes plus anciens de l'hôpital et les équipements médicaux auxquels il n'est pas possible d'appliquer des correctifs, limitez le risque en implémentant une technologie de listes blanches d'applications qui verrouille les systèmes et empêche l'exécution de programmes non autorisés. Isolez ces systèmes et équipements du reste du réseau à l'aide d'un pare-feu ou d'un système de prévention des intrusions. Désactivez les ports et les services superflus sur ces systèmes pour limiter les points d'entrée possibles d'une infection.
- Protégez les terminaux. Utilisez une solution de protection des terminaux et ses fonctionnalités avancées. Souvent, les clients se limitent à certaines fonctionnalités activées par défaut à l'installation. L'implémentation de certaines fonctions avancées (tel le blocage de l'exécution des fichiers exécutables à partir du dossier Temp) permet de détecter et de stopper davantage de logiciels malveillants.
- Si possible, évitez de stocker des données sensibles sur des disques locaux. Demandez aux utilisateurs de les stocker sur des lecteurs réseau sécurisés. Vous limitez ainsi le temps d'arrêt car il est possible de simplement restaurer une image des systèmes infectés.
- Utilisez des logiciels antispam. La première étape de la plupart des campagnes de ransomware est l'envoi d'un e-mail de phishing contenant un lien ou une pièce jointe. Dans le cas où la pièce jointe contenant le logiciel de demande de rançon est un fichier .scr ou un fichier d'un autre format peu courant, il est possible de la bloquer simplement en configurant une règle de filtrage antispam. Si vous autorisez les fichiers .zip, veillez à ce que leur analyse porte sur deux niveaux d'imbrication au moins pour détecter tout contenu malveillant potentiel.
- Bloquez les programmes et le trafic indésirables ou inutiles. Si vous n'avez pas besoin de l'application Tor, bloquez-la de même que le trafic réseau lié à celle-ci. Souvent, cela empêchera le ransomware d'obtenir la clé publique RSA du serveur de contrôle et, par conséquent, l'exécution de son processus de chiffrement.
- Segmentez votre réseau pour les systèmes critiques essentiels aux soins des patients.
- Isolez vos sauvegardes. Assurez-vous que les systèmes, le stockage et les bandes de sauvegarde sont conservés dans un endroit inaccessible aux systèmes des réseaux de production. Si la charge active des attaques de ransomware se propage latéralement, elle pourrait affecter les données sauvegardées.
- Implémentez une infrastructure virtuelle pour les systèmes de gestion des dossiers médicaux électroniques critiques qui sont isolés du reste du réseau de production.
- Sensibilisez régulièrement vos utilisateurs à la problématique de la sécurité. Cette formation continue est capitale, dans la mesure où la plupart des attaques par logiciel de demande de rançon débutent par l'envoi d'e-mails de phishing. Les statistiques prouvent que, sur dix e-mails envoyés par les auteurs d'attaques, au moins un fera mouche. N'ouvrez pas des e-mails et des pièces jointes si leur expéditeur vous est inconnu ou sans avoir vérifié son identité.

Comment les technologies Intel Security vous aident à vous protéger contre les logiciels de demande de rançon

McAfee VirusScan Enterprise et McAfee Endpoint Security 10

- Si vous disposez de McAfee VirusScan Enterprise (VSE) ou McAfee Endpoint Security (ENS), appliquez les mesures suivantes :
  - Utilisez McAfee ePolicy Orchestrator (ePO) quotidiennement pour déployer des fichiers de signature (DAT) actualisés.
  - Assurez-vous que McAfee Global Threat Intelligence (McAfee GTI) est activé, dans la mesure où ce système contient plus de 7 millions de signatures de ransomware uniques.
  - Élaborez des règles de protection de l'accès pour bloquer l'installation et les charges actives des ransomwares. Pour ce faire, reportez-vous aux articles de la base de connaissances KB81095 et KB54812.
  - Utilisez des règles de confinement dynamique d'applications pour empêcher les applications inconnues d'effectuer des opérations malveillantes.

McAfee Threat Intelligence Exchange

- Configurez les stratégies suivantes pour McAfee Threat Intelligence Exchange (TIE) :
  - Commencez par activer le mode d'observation.
  - À mesure que des processus suspects sont identifiés sur les terminaux, utilisez des marqueurs système pour appliquer les stratégies de mise en œuvre de McAfee TIE.
  - Nettoyez au niveau de réputation « 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 du Serveur TIE : Pour les fichiers qui n'ont pas encore été soumis à McAfee TIE, acceptez les réputations McAfee ATD.
- Intervention manuelle de McAfee Threat Intelligence Exchange :
  - Appliquez les règles en matière de réputation des fichiers (selon le mode de fonctionnement).
  - Fichiers vraisemblablement malveillants : nettoyage/suppression.
  - Fichiers susceptibles d'être malveillants : blocage.
  - Des règles de réputation d'entreprise (organisationnelles) peuvent remplacer McAfee GTI. Vous pouvez choisir de bloquer un processus indésirable, par exemple une application non prise en charge ou vulnérable. Marquez le fichier comme potentiellement malveillant (option « Might be malicious »).
  - Intégrez les données de réputation provenant de sources externes dans McAfee TIE à l'aide d'indicateurs de compromission.

McAfee Advanced Threat Defense

- McAfee Advanced Threat Defense intègre les fonctionnalités de détection suivantes :
  - Détection basée sur les signatures : McAfee Labs dispose actuellement de plus de 150 millions de signatures, 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 signature.
  - Règles YARA personnalisées.
  - Analyse statique complète du code : reconstitue la logique du code pour évaluer les attributs et les jeux d'instructions, 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, dont Windows 7, Windows 8 et Windows XP
  - applications Windows installées (Word, Excel) avec macros activées
- Créez des profils d'analyseur uniques avec accès Internet pour les différents systèmes d'exploitation :
  - De nombreux échantillons exécutent un script à partir d'un document Microsoft Office, qui établit une connexion sortante et active le logiciel malveillant. La mise à disposition d'un profil d'analyseur avec accès Internet améliore les taux de détection.

McAfee Application Control

- McAfee Application Control assure la protection au moyen de listes blanches d'applications. Cette solution est particulièrement adaptée aux équipements suivants :
  - Équipement statiques tels que les appareils médicaux
  - Systèmes dotés d'anciennes versions des systèmes d'exploitation qui ne font plus l'objet de mises à jour
  - Serveurs d'applications assurant un nombre limité de services
  - Systèmes faisant rarement l'objet de modifications
- Installation initiale
  - McAfee Application Control analyse l'intégralité du système au moment de l'installation et dresse un inventaire des terminaux, ainsi que des applications à mettre sur liste blanche.
- Mode d'observation
  - Permet aux administrateurs de surveiller les nouvelles applications installées ou lancées. Une option permet en outre de les ajouter à la liste blanche centralisée dès lors qu'il a été établi qu'elles sont autorisées.
  - Identifie les nouveaux outils de mise à jour des applications approuvés au sein de l'environnement, pour faciliter l'enregistrement sur liste blanche.
  - Identifie les méthodes de mise à jour de la liste blanche, telles que les processus, les certificats, les répertoires ou les utilisateurs approuvés.
- Mode d'approbation automatique
  - Les utilisateurs ont la possibilité d'approuver des applications qui ne figurent pas dans la liste blanche. Cette option permet une certaine flexibilité et réduit l'impact sur les activités.
  - Les administrateurs peuvent surveiller le contenu approuvé par l'utilisateur de manière centralisée, de même qu'accepter des applications ou révoquer les autorisations en fonction de la réputation et des stratégies de l'entreprise.
- Mise en œuvre d'une liste blanche
  - Le système bénéficie d'une protection totale contre les applications inconnues, notamment les applications malveillantes telles que le ransomware.
  - Les utilisateurs finaux reçoivent une notification avec la procédure à suivre pour approuver de nouveaux fichiers exécutables.

Lectures complémentaires

Communauté Intel Security Expert Center

- McAfee VirusScan Enterprise
- McAfee Endpoint Security
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee Application Control

916_0816_brf_protecting-health-care-systems-ransomware

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