Présentation de solution

Protection contre les menaces stéganographiques

La stéganographie est l'art de la dissimulation de messages secrets. Ellexpeut s'employer dans le monde numérique pour cacher des informations dans une image, une piste audio, un clip vidéo ou un fichier texte. Même si elle peut avoir des fins légitimes, elle est le plus souvent exploitée par des logiciels malveillants.

En effet, pour éviter d'être détectés, certains malwares recourent à la stéganographie numérique pour dissimuler leur contenu malveillant dans un fichier en apparence insignifiant, le « fichier de couverture ». Cette technique de contournement s'appuie sur le fait que, pour identifier un contenu dangereux, la plupart des signatures antimalware sont conçues pour examiner le fichier de configuration du logiciel malveillant. Avec la stéganographie, ce dernier est incorporé dans le fichier de couverture. De plus, le stégo-fichier ainsi obtenu peut être déchiffré dans la mémoire principale, ce qui réduit encore la probabilité de détection. Enfin, il est extrêmement difficile de repérer la présence d'informations cachées (fichier de configuration, mise à jour de fichier binaire, commande de robot, etc.) dans un stégo-fichier. Malheureusement, l'utilisation de la stéganographie dans le cadre de cyberattaques est aussi facile à mettre en œuvre que difficile à détecter.

Stratégies et procédures de protection contre les attaques stéganographiques

McAfee recommande aux entreprises de prendre les mesures suivantes pour se défendre contre les menaces stéganographiques.

- **Renforcer la sécurité des mécanismes de fourniture et de distribution de logiciels utilisés pour assurer la protection contre les menaces internes.** Il est toujours conseillé de disposer d'un référentiel central d'applications d'entreprise approuvées, à partir duquel les utilisateurs peuvent télécharger des logiciels autorisés. De cette façon, vous éviterez les risques liés au téléchargement de logiciels à partir de sources inconnues susceptibles de contenir du code sténographique.

McAfee™
Together is power.

- **Examiner soigneusement les images.** Au moyen d'un logiciel de retouche d'image, recherchez les marqueurs de la stéganographie, tels que de légères différences de couleur dans les images. La présence d'un grand nombre de couleurs dupliquées dans une image peut également indiquer une attaque stéganographique.
- **Contrôler l'utilisation des logiciels stéganographiques.** Leur présence sur un système d'entreprise doit être interdite, à moins qu'elle ne soit spécifiquement requise à des fins professionnelles. Déployez-les uniquement dans un segment de réseau isolé.
- **N'autoriser que les signatures approuvées.** Installez uniquement des applications dotées de signatures approuvées et proposées par des fournisseurs de confiance.
- **Configurer une solution antimalware pour détecter les binders.** Les logiciels antimalware doivent être configurés de sorte à pouvoir déceler la présence de binders susceptibles de contenir des stégo-images.
- **Segmenter le réseau.** Au cas où votre entreprise serait victime d'une attaque stéganographique, une architecture de virtualisation approuvée associée à une segmentation de réseau adéquate est utile pour endiguer la propagation. En effet, la surveillance continue du trafic et le processus de démarrage sûr et vérifiable que cette architecture utilise permettent de mieux isoler les applications.
- **Surveiller le trafic sortant.** Vous pourrez ainsi identifier les attaques stéganographiques abouties.

Comment les produits McAfee peuvent vous protéger contre les menaces stéganographiques

McAfee Endpoint Security

Prévention contre les menaces

Veillez à configurer McAfee Endpoint Security (ENS) de manière à bloquer les logiciels malveillants connus susceptibles de contenir du code stéganographique :

- Maintenez McAfee ENS parfaitement à jour en déployant systématiquement les patchs, les versions de fichiers DAT et le moteur d'analyse les plus récents.
- Veillez à ce que tous les systèmes de votre environnement soient protégés et à jour.
- Configurez l'analyse en temps réel (à l'accès) de telle sorte que tous les fichiers soient examinés lors de la lecture et lors de l'écriture. Ne désactivez jamais le paramètre d'analyse « lors de la lecture », sauf lors de la configuration de stratégies pour les processus à risque faible.
- Les règles d'exclusion de l'analyse doivent être limitées autant que possible et utilisées uniquement lorsque c'est nécessaire. Si vous suspectez la présence d'un logiciel malveillant, assurez-vous que toute exclusion de l'analyse est temporairement désactivée. Consultez l'article KB88595 de la base de connaissances pour en savoir plus sur la définition d'exclusions.
- Informez-vous sur les implications pour les performances des options de configuration Processus à haut risque / Processus par défaut / Processus à faible risque visant à limiter votre exposition aux menaces stéganographiques si votre environnement est fortement sollicité ou que sa sécurité par matériel est rudimentaire. Pour en savoir plus sur l'optimisation des performances avec McAfee Endpoint Security, consultez l'article KB88205 de la base de connaissances.
- Configurez McAfee ENS pour qu'il utilise la fonctionnalité de réputation des fichiers de McAfee Global Threat Intelligence (GTI). Cette technologie contribue à combler la brèche entre les menaces de type « jour zéro » et les fonctions de détection basées sur les signatures. Pour en savoir plus sur les paramètres recommandés pour la fonctionnalité de réputation des fichiers de McAfee GTI, consultez l'article KB74983 de la base de connaissances. Vous trouverez également des informations complémentaires dans l'article KB53735.

- Configurez les règles de protection de l'accès de McAfee ENS de façon à empêcher la création de fichiers autorun.inf.
- Utilisez les règles de protection de l'accès pour bloquer l'installation des menaces inconnues.

Contrôle Web

Le module Contrôle Web de McAfee ENS s'appuie sur les services de catégorisation et de réputation des sites web de McAfee GTI. Les logiciels infectés par des menaces stéganographiques se dissimulent souvent sur des sites de distribution de malwares.

Le module Contrôle Web de McAfee ENS identifie les sites qui hébergent des logiciels malveillants, sont infectés par ceux-ci ou contiennent du contenu inapproprié, et vous avertissent avant que vous n'y accédiez.

Avantages du module Contrôle Web

- Il renseigne par des icônes et un code couleur le degré de sécurité relatif des sites web :
  - Vert = sûr (risque très faible ou nul)
  - Jaune = attention (risque mineur)
  - Rouge = avertissement (risque grave)
  - Gris = inconnu (site non encore évalué, à visiter avec prudence)
  - McAfee Secure = site évalué quotidiennement en termes de risques de piratage
- Il peut être déployé et configuré facilement à l'aide de McAfee ePolicy Orchestrator.
- Il procure un niveau de protection supplémentaire pour les terminaux. La solution peut être utilisée avec Internet Explorer, Firefox et Chrome.
- Il assure une protection antispam efficace pour empêcher les e-mails malveillants de pénétrer dans le réseau.

En savoir plus : Guide produit McAfee Endpoint Security - Utilisation du module Contrôle Web

Protection adaptative contre les menaces

- Activez McAfee Real Protect pour appliquer des techniques d'apprentissage automatique (machine learning) dans le but d'identifier les menaces avancées en s'appuyant à la fois sur leurs caractéristiques, sur leurs activités potentielles (analyse pré-exécution) et sur leurs actions réelles (analyse comportementale dynamique). Le tout sans signatures. En savoir plus : Protection adaptative contre les menaces — Real Protect
- Appliquez l'option de confinement d'application dynamique et suivez les meilleures pratiques recommandées. En savoir plus : KB87843.

McAfee VirusScan Enterprise

Les clients qui ne disposent pas de la dernière version de McAfee ENS doivent veiller à configurer McAfee VirusScan Enterprise (VSE) de manière à bloquer les logiciels malveillants connus susceptibles de contenir du code stéganographique :

- Maintenez McAfee VSE parfaitement à jour en déployant systématiquement les patchs, les versions de fichiers DAT et le moteur d'analyse les plus récents.
- Veillez à ce que tous les systèmes de votre environnement soient protégés et à jour.
- Configurez l'analyse en temps réel (à l'accès) de telle sorte que tous les fichiers soient examinés lors de la lecture et lors de l'écriture. Ne désactivez jamais le paramètre d'analyse « lors de la lecture », sauf lors de la configuration de stratégies pour les processus à risque faible.

- Les règles d'exclusion de l'analyse doivent être limitées autant que possible et utilisées uniquement lorsque c'est nécessaire. Si vous suspectez la présence d'un logiciel malveillant, assurez-vous que toute exclusion de l'analyse est temporairement désactivée. Consultez l'article KB50998 de la base de connaissances pour en savoir plus sur la définition d'exclusions.
- Si votre environnement est fortement sollicité ou que sa sécurité par matériel est rudimentaire, utilisez les configurations de stratégies Processus à haut risque / Processus par défaut / Processus à faible risque de manière à limiter votre exposition aux menaces stéganographiques. Pour comprendre cette fonction et apprendre à la configurer, lisez respectivement les articles KB55139 et KB58692 de la base de connaissances.
- Configurez McAfee VSE pour qu'il utilise la fonctionnalité de réputation des fichiers de McAfee Global Threat Intelligence (GTI). Cette technologie contribue à combler la brèche entre les menaces de type « jour zéro » et les fonctions de détection basées sur les signatures. Pour en savoir plus sur les paramètres recommandés pour la fonctionnalité de réputation des fichiers de McAfee GTI, consultez l'article KB74983 de la base de connaissances. Vous trouverez également des informations complémentaires dans l'article KB53735.
- Configurez les règles de protection de l'accès de McAfee VSE de façon à empêcher la création de fichiers autorun.inf.
- Utilisez les règles de protection de l'accès pour bloquer l'installation des menaces inconnues.

McAfee Application Control
McAfee Application Control permet de bloquer efficacement les applications et le code non autorisés sur les serveurs, les postes de travail d'entreprise et les équipements à fonction fixe en cas d'attaque stéganographique. McAfee Application Control empêche la compromission des fichiers et la propagation des infecteurs de fichiers sur le réseau.

McAfee Application Control assure deux types de protections essentielles :

- **Protection basée sur les fichiers.** La solution repousse les attaques qui se dissimulent dans les fichiers, un comportement caractéristique des menaces stéganographiques. Ces attaques peuvent tenter d'exécuter de nouvelles applications ou de modifier les applications déjà installées.
- **Protection de la mémoire.** La solution bloque également les attaques basées en mémoire, qui peuvent être transmises par Internet, via le réseau ou en local à la suite de l'exécution d'un fichier.

Protection basée sur les fichiers
Les programmes qui ne figurent pas dans la liste blanche ne sont ni autorisés, ni protégés. À l'inverse, ceux qui sont placés sur la liste blanche sont à la fois autorisés et protégés. Grâce à cette protection, si une application non autorisée est introduite sur un terminal (au moyen d'un téléchargement, d'un accès sur le réseau, en local via une clé USB ou un CD, etc.), elle peut être copiée sur ce terminal ou modifiée et déplacée d'un dossier à l'autre, mais en aucun cas elle ne pourra être exécutée. Des exemples d'événements de ce type sont décrits ci-dessous.

Exécution refusée	Lorsqu'une application qui n'est pas présente sur la liste blanche tente de s'exécuter, elle est bloquée par McAfee Application Control.
Installation d'ActiveX bloquée	McAfee Application Control empêche toute tentative d'installation de contrôles ActiveX non autorisés.

Si un processus non autorisé (qui émane d'un fichier malveillant s'exécutant sur un terminal distant, p. ex.) ou un utilisateur non autorisé essaie de modifier, renommer, déplacer ou supprimer un fichier placé sur liste blanche (et donc protégé), McAfee Application Control bloque l'opération. Des exemples d'événements de ce type sont décrits ci-dessous.

Écriture du fichier refusée	McAfee Application Control empêche tout processus non autorisé de modifier des applications figurant sur la liste blanche.
Modification du package interdite	Dans le cas d'une application qui utilise un package d'installation MSI, McAfee Application Control bloque les tentatives d'installation, de modification et de suppression effectuées à l'aide d'un mécanisme non autorisé.

En savoir plus : McAfee Application Control — Guide des meilleures pratiques

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) recourt à une approche multiniveau innovante pour détecter les programmes de compression (packers) très sophistiqués et furtifs, les charges actives chiffrées et les logiciels malveillants de type « jour zéro ». La solution combine des signatures de malware à faible empreinte, l'analyse de la réputation et l'émulation en temps réel avec des fonctions d'analyse de code statique et dynamique (sandboxing) pour décortiquer le comportement réel des logiciels malveillants.

En savoir plus : McAfee Advanced Threat Defense — Questions fréquentes

Autres lectures conseillées

Centre de conseil sur la sécurité McAfee : Protection contre le phishing

Tableau de bord du paysage des menaces : Le kit d'exploit Sundown a été mis à jour fin 2016 et des recherches ont révélé qu'il utilisait la stéganographie pour dissimuler son code d'exploit.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/fr