Présentation de solution

Protection contre les logiciels malveillants furtifs

Comme nous l'avons expliqué dans le Rapport sur le paysage des menaces de McAfee Labs — Juin 2017, les logiciels malveillants emploient de nombreuses techniques de contournement pour échapper à la détection. Ils exploitent ou parasitent des applications légitimes. Ils peuvent déterminer lorsqu'ils sont analysés dans un environnement sandbox et reporter leur exécution, patientant des jours, des semaines, voire des mois, avant de passer à l'attaque.

Un dispositif de sécurité capable de contrer ces techniques repose sur trois piliers.

- **Ressources humaines** : Les professionnels de la sécurité doivent être correctement formés pour intervenir de façon efficace en cas d'incident de sécurité et gérer correctement les technologies de sécurité actuelles. Les cybercriminels n'hésitent pas à recourir à l'ingénierie sociale pour infecter les utilisateurs. Sans formation et sensibilisation au problème, les utilisateurs risquent d'ouvrir la porte aux pirates informatiques.
- **Processus** : Des structures et des processus internes clairement définis doivent être mis en place pour garantir l'efficacité des professionnels de la sécurité. L'adoption de bonnes pratiques de sécurité (mises à jour, sauvegardes, cyberveille, plans d'intervention sur incident, etc.) est essentielle et garante de l'efficacité de l'équipe de sécurité.
- **Technologies** : Les technologies soutiennent l'équipe et les processus. Elles doivent actualisées et optimisées afin de s'adapter aux nouvelles menaces.

Des politiques et procédures exploitables pour se protéger des logiciels malveillants furtifs

- Les utilisateurs représentent la première défense contre les infections par des logiciels malveillants. Ceux-ci doivent connaître le risque lié au téléchargement et à l'installation d'applications émanant de sources potentiellement dangereuses. Ils doivent également savoir que les malwares peuvent être téléchargés à leur insu au cours de leur navigation web.
- Les navigateurs web et les modules complémentaires doivent toujours être à jour. De même, les solutions antimalware sur les terminaux et les passerelles réseau doivent être mises à jour et à niveau pour disposer des versions les plus récentes.

McAfee™
Together is power.

- Les systèmes qui ne sont pas distribués et certifiés par le service de sécurité informatique de l'entreprise ne doivent pas être autorisés sur le réseau approuvé. Les logiciels malveillants furtifs peuvent être facilement propagés par des systèmes non sécurisés connectés au réseau approuvé de l'entreprise.
- Ces menaces peuvent se dissimuler au sein de logiciels légitimes qui ont été précédemment infectés par des chevaux de Troie. Pour parer à des attaques de ce type, nous recommandons des mécanismes de distribution de logiciels stricts. Il est toujours intéressant de posséder un référentiel central d'applications d'entreprise à partir duquel les utilisateurs peuvent télécharger des logiciels approuvés.
- Lorsque les utilisateurs sont autorisés à installer des applications qui n'ont pas été préalablement validées par l'équipe de sécurité informatique, sensibilisez les utilisateurs au fait que seules les applications possédant des signatures approuvées d'éditeurs connus peuvent être installées. Il arrive souvent que des applications proposées en ligne, à l'apparence inoffensive, soient infectées par des logiciels malveillants furtifs.
- Évitez de télécharger des applications à partir d'autres types de sources que des sources web. Le risque de télécharger des logiciels infectés à partir de groupes Usenet, de canaux IRC, de clients de messagerie instantanée ou de réseaux peer-to-peer est très élevé. Les liens renvoyant à des sites web dans les canaux IRC et la messagerie instantanée pointent souvent vers des fichiers à télécharger infectés.
- Mettez en place un programme de formation sur la prévention des attaques de phishing. Les logiciels malveillants sont fréquemment distribués par les attaques de phishing.
- Tirez parti des flux de cyberveille associés à des technologies antimalware. Leur utilisation conjointe permet d'accélérer la détection des menaces.

Comment les produits McAfee peuvent protéger contre les logiciels malveillants furtifs

McAfee propose une nouvelle génération de fonctionnalités de sécurité, conçues pour combattre les menaces modernes les plus furtives. En tirant parti d'outils puissants d'analyse basée sur l'apprentissage automatique et de confinement des applications, les entreprises peuvent débusquer les menaces cachées et les arrêter net, beaucoup plus rapidement et avec moins d'efforts.

Ces fonctionnalités sont disponibles dans les produits McAfee suivants :

Real Protect

Real Protect, inclus dans la solution McAfee Endpoint Protection, combine analyse statique pré-exécution et analyse comportementale post-exécution pour bloquer davantage de logiciels malveillants que n'importe quelle autre solution d'analyse exclusivement statique ou basée sur les signatures, les deux étant intégrées dans l'écosystème de sécurité McAfee. Il applique des techniques poussées d'apprentissage automatique (machine learning) pour identifier le code malveillant en évaluant ses fonctionnalités statiques (analyse pré-exécution) et son comportement réel (analyse comportementale dynamique) — le tout sans signatures. Real Protect décortique les dernières techniques de dissimulation pour démasquer les menaces furtives afin que les logiciels malveillants n'aient nulle part où se cacher.

Confinement d'application dynamique

Le confinement d'application dynamique, fonctionnalité également incluse dans la solution McAfee Endpoint Protection, protège les terminaux « patient zéro » contre des infections par des logiciels malveillants « jour zéro ». Lorsqu'un terminal détecte un fichier malveillant, le confinement d'application dynamique bloque immédiatement les comportements révélateurs d'un logiciel malveillant (modification du Registre, écriture dans un répertoire temporaire ou suppression de fichiers). À la différence d'autres techniques qui retiennent le fichier (et l'utilisateur) pendant la durée de l'analyse, le confinement d'application dynamique laisse le fichier suspect se charger en mémoire sans lui permettre d'apporter des modifications au terminal ni d'infecter d'autres systèmes tant que tout soupçon n'a pas été écarté.

Real Protect et le confinement d'application dynamique sont intégrés entre eux, mais aussi avec McAfee Endpoint Protection et avec des solutions de sécurité d'autres éditeurs telles que SPLUNK, Avecto, ForeScout — pour offrir une défense multiniveau contre les menaces les plus furtives. Ces fonctionnalités donnent à votre équipe de sécurité la possibilité de contrôler toutes les étapes du cycle de défense contre les menaces — la détection, la correction et la protection proactive — de façon rapide et automatisée.

Vous pouvez tirer parti de Real Protect et du confinement d'application dynamique pour :

- Débusquer davantage d'attaques en perçant à jour les techniques de dissimulation pour voir toutes les menaces.
- Limiter l'impact d'une attaque : Vous confinez, protégez et prévenez tout dommage aux systèmes, avant que l'attaque survienne ou qu'elle puisse causer des dommages irréversibles.
- Bénéficier d'un suivi et adapter vos défenses : Vous utilisez des défenses intégrées et automatisées pour effectuer un éventail plus large d'opérations de sécurité de façon automatique, sans devoir les activer manuellement.

Regardez une vidéo de démonstration pour découvrir comment fonctionnent Real Protect et le confinement d'application dynamique.

Meilleures pratiques de configuration du confinement d'application dynamique
Les règles de confinement d'application dynamique définies dans la stratégie McAfee Default se limitent au signalement des applications suspectes, ce qui réduit le nombre de faux positifs. Le module Protection adaptative contre les menaces offre deux autres stratégies de confinement prédéfinies : McAfee Default Balanced et McAfee Default Security. Ces stratégies définissent les règles recommandées pour le blocage, sur la base du profil de sécurité :

- McAfee Default Balanced (Stratégie par défaut, équilibrée) offre un niveau de protection de base tout en limitant le nombre de faux positifs pour de nombreux programmes d'installation et logiciels non signés courants.
- McAfee Default Security (Stratégie par défaut, sécurité renforcée) offre une protection plus stricte mais est susceptible de générer davantage de faux positifs pour des programmes d'installation et applications non signés.

Évaluez l'impact des règles de confinement d'application dynamique en utilisant la stratégie McAfee Default avec des règles définies pour le signalement uniquement. Pour déterminer s'il convient de définir des règles de blocage, surveillez les journaux et les rapports. Après avoir collecté des événements de type « infraction aux règles de confinement autorisée » (ID d'événement 37280), définissez des réputations et des exclusions de confinement au niveau de l'entreprise avant de mettre en œuvre la stratégie McAfee Default Balanced.

Le confinement d'application dynamique peut exclure certains processus sur la base de leur nom, hachage MD5, données de signature et chemin d'accès. Si votre entreprise signe des outils déployés en interne, ajoutez ces signatures aux exclusions pour réduire le nombre de faux positifs.

Les règles de confinement possèdent une option de contrôle du volume qui limite le nombre d'événements générés (une fois par heure, par règle et par processus). Le contrôle du volume surveille les processus en fonction de leur ID. Lorsqu'un processus redémarre, le système d'exploitation lui attribue un nouvel ID, ce qui réinitialise le contrôle du volume, même si le nom du processus reste le même. Si, par exemple, le processus A enfreint la règle de confinement A 100 fois par heure, vous recevrez un seul événement toute les heures. Si le processus A redémarre pendant l'heure en question, le contrôle du volume est réinitialisé pour ce processus et vous recevrez un nouvel événement s'il continue à enfreindre la règle A. Si le processus B enfreint la même règle A, vous recevrez un second événement (avec des détails relatifs au processus B). Lisez cet article pour en savoir plus sur les meilleures pratiques à respecter concernant les règles de confinement d'application dynamique définies par McAfee.

Exécutez l'outil GetClean de McAfee sur les images de base des systèmes de production de votre déploiement pour garantir l'envoi de fichiers non infectés à McAfee Global Threat Intelligence (GTI) à des fins de classification. Grâce à cet outil, vous avez l'assurance que McAfee GTI ne génère pas une valeur de réputation erronée pour vos fichiers. Pour plus d'informations, consultez le guide produit de GetClean (PD23191).

McAfee Cloud Threat Detection

McAfee Cloud Threat Detection (CTD) optimise les solutions de protection de McAfee en déterminant la dangerosité des logiciels malveillants avancés et en exposant les menaces. Demandez un compte McAfee ePO Cloud, activez McAfee CTD et intégrez-le avec vos produits McAfee.

Pour utiliser les fonctionnalités de McAfee Cloud Threat Detection (CTD) avec vos produits de sécurité McAfee, procédez comme suit :

- Activez McAfee CTD dans la console McAfee ePO Cloud.
- Activez McAfee CTD dans l'interface de votre produit de sécurité McAfee et récupérez la clé de provisionnement.
- Utilisez cette clé de provisionnement pour générer une clé d'activation dans l'interface McAfee ePO Cloud.
- La clé d'activation vous servira à activer votre produit de sécurité McAfee.

Les instructions pour obtenir la clé de provisionnement et activer un produit varient d'un produit à l'autre. Reportez-vous au guide produit pour obtenir des instructions détaillées sur l'intégration de McAfee CTD avec votre produit McAfee.

Lorsque les produits intégrés commencent à envoyer les fichiers à McAfee CTD pour analyse, vous pouvez consulter vos informations d'utilisation dans la page Abonnements de la console McAfee ePO Cloud.

McAfee Active Response

- McAfee Active Response est conçu pour détecter et répondre aux 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 peuvent être recherchées et éliminées avant qu'elles n'aient l'occasion de se propager.
- Les collecteurs personnalisés permettent de créer des outils spécifiques afin de rechercher et d'identifier les indicateurs de compromission associés aux applications infectées par des chevaux de Troie.
- L'utilisateur peut intégrer 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 spécifiques sont détectés, une action de suppression peut être automatiquement exécutée.

Autres lectures conseillées

Neutralize Advanced Threats: Adapt Layered Defenses for Comprehensive Malware Protection (Neutralisation des menaces avancées : Adaptation des défenses multiniveau pour garantir une protection complète contre les logiciels malveillants)

Centre de conseil sur la sécurité de McAfee : Les 10 meilleurs moyens de se prémunir contre les chevaux de Troie et les logiciels malveillants (malwares)

McAfee Endpoint Security : Questions fréquentes (FAQ)

McAfee
Together is power.

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