Présentation de solution

Protection contre les logiciels malveillants sans fichier

Le ***Rapport de McAfee® Labs sur le paysage des menaces — Novembre 2015*** se penche sur les logiciels malveillants sans fichier. Il propose une analyse technique détaillée de Kovter, une menace qui échappe à la détection en limitant ou en éliminant tout stockage de fichiers binaires sur disque pour dissimuler son code dans le Registre d'un hôte compromis. Les auteurs de logiciels malveillants compliquent la détection par des techniques qui renforcent l'efficacité des attaques, telles que le polymorphisme, les fonctions de surveillance, la révocation des autorisations, etc. En 2015, nous avons également observé des attaques tirant parti de fonctions comme l'infrastructure de gestion Windows (WMI, Windows Management Instrumentation) et Windows PowerShell pour compromettre des terminaux sans jamais enregistrer de fichier binaire sur disque — ce qui les rend très difficiles à identifier.

Les infections sans fichier résidentes en mémoire sont connues depuis longtemps des experts en sécurité informatique. Bien qu'elles aient été considérées comme des logiciels malveillants sans fichier, les familles antérieures déposaient malgré tout un petit fichier binaire sur le disque au cours de l'attaque initiale, avant de migrer vers la mémoire principale de l'hôte compromis. Par contre, les dernières techniques de contournement utilisées par les logiciels malveillants sans fichier (p. ex. Kovter, Powelike et XswKit) ne laissent aucune trace sur le disque. Cette nouvelle méthodologie complique singulièrement la détection dans la mesure où celle-ci se base généralement sur la présence de fichiers statiques sur disque.

Ces logiciels malveillants sont généralement de trois types :

- **Résident en mémoire** — Ce type de logiciel malveillant sans fichier utilise l'espace mémoire d'un fichier Windows légitime. Il charge son code dans cet espace mémoire et y réside jusqu'à ce qu'il soit accédé ou activé. Bien que l'exécution intervienne au sein de l'espace mémoire du fichier légitime, il existe un fichier physique dormant qui initie ou redémarre l'exécution. Par conséquent, ce type de logiciel malveillant n'est pas complètement « sans fichier ».
- **Rootkit** — Certains logiciels malveillants sans fichier dissimulent leur présence derrière une interface de programmation d'application (API) utilisateur ou noyau. Un fichier est présent sur le disque mais en mode furtif.

intel Security

- **Registre Windows —** Certains types de logiciels malveillants récents résident dans le Registre du système d'exploitation Microsoft Windows. Leurs auteurs ont exploité des fonctionnalités tel le cache de miniatures Windows, utilisé afin de stocker des images pour l'affichage Miniatures de l'Explorateur Windows. Le cache de miniatures offre au logiciel malveillant un mécanisme de persistance. Les logiciels malveillants de ce type doivent toujours pénétrer dans le système de la victime via un fichier binaire statique. La plupart d'entre eux utilisent l'e-mail comme vecteur. Dès que l'utilisateur clique sur la pièce jointe, le logiciel malveillant écrit l'intégralité du fichier de la charge active sous une forme chiffrée dans une ruche du Registre Windows. Ensuite, il s'autodétruit pour disparaître du système.

Très intelligemment conçues, les familles de logiciels malveillants sans fichier comme Kovter, Powelike et XswKit peuvent exécuter des attaques du Registre Windows sans le moindre fichier et sans laisser aucune trace dans le système de fichiers. Bien que leurs auteurs préparent l'environnement destiné à lancer ces attaques en exécutant du code dans un fichier, ce dernier s'autodétruit dès que le système est prêt pour l'attaque malveillante.

Comment Intel Security peut vous aider à vous protéger contre les logiciels malveillants sans fichier

La détection de logiciels malveillants qui n'installent pas de fichier binaire initial peut s'avérer difficile et n'est souvent possible qu'après enquête des équipes de sécurité. Toutefois, la mise en place de contrôles appropriés pour fermer la porte aux attaquants joue un rôle crucial dans le blocage de ce type de menaces.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense est une solution multiniveau de détection des logiciels malveillants qui combine divers moteurs d'inspection. Grâce à plusieurs moteurs appliquant une inspection basée sur les signatures et la réputation, l'émulation en temps réel, l'analyse statique complète du code et l'analyse dynamique en environnement restreint (sandbox), McAfee Advanced Threat Defense garantit une protection contre les logiciels malveillants qui déposent initialement un fichier binaire sur le système pris pour cible.

- **Détection basée sur les signatures** — Débusque les virus, les vers, les logiciels espions, les robots, les chevaux de Troie, les débordements de mémoire tampon et les attaques combinées. La solution utilise une base de connaissances exhaustive créée et gérée par McAfee Labs.
- **Détection basée sur la réputation** — Tire parti du service McAfee Global Threat Intelligence (McAfee GTI) pour analyser la réputation des fichiers afin de détecter les nouvelles menaces émergentes.
- **Émulation et analyse statique en temps réel** — Permet de détecter rapidement les logiciels malveillants et les menaces « jour zéro » non identifiables au moyen des techniques basées sur les signatures ou la réputation.
- **Analyse statique complète du code** — Reconstitue la logique du code pour évaluer l'ensemble des attributs et des jeux d'instructions, et effectuer un examen approfondi du code source sans l'exécuter. En ouvrant tous les types de fichiers compressés afin d'effectuer une analyse minutieuse et une classification des logiciels malveillants qu'ils contiennent, les fonctionnalités de décompression permettent aux entreprises de mieux comprendre les risques posés par les logiciels malveillants auxquels elles ont affaire.
- **Analyse dynamique dans un environnement restreint de type « sandbox »** — En présence d'un fichier dont les moteurs d'inspection ci-dessus sont incapables de déterminer l'innocuité, McAfee Advanced Threat Defense offre la possibilité d'exécuter son code dans un environnement d'exécution virtuel et d'observer ainsi son comportement. Les environnements virtuels peuvent être configurés de façon à correspondre à ceux des hôtes cibles. McAfee Advanced Threat Defense prend en charge des images personnalisées des systèmes d'exploitation Windows XP SP2 et SP3, Windows 7 (32 et 64 bits), Windows 8 (32 et 64 bits), Windows Server 2003, Windows Server 2008 (64 bits) ainsi qu'Android.

McAfee Threat Intelligence Exchange

Une plate-forme de cyberveille capable de s'adapter aux besoins de l'environnement au fil du temps constitue un outil de première importance. **McAfee Threat Intelligence Exchange** réduit considérablement les risques d'attaques menées à l'aide de logiciels malveillants sans fichier, grâce à la visibilité qu'il offre sur les menaces immédiates, notamment les applications ou fichiers inconnus exécutés dans l'environnement.

- **Cyberveille complète sur les menaces** — Créez aisément une base personnalisée de cyberveille enrichie par plusieurs sources mondiales. Il est possible de combiner les flux McAfee GTI ou des flux externes avec des informations locales sur les menaces, issues de données d'événements historiques et en temps réel fournies par les solutions de sécurité des terminaux, de passerelle, etc.
- **Prévention de l'exécution et correction** — McAfee Threat Intelligence Exchange peut intervenir pour empêcher l'exécution d'applications inconnues dans l'environnement. Si une application dont l'exécution était auparavant autorisée se révèle par la suite malveillante, McAfee Threat Intelligence Exchange peut, grâce à ses fonctions de gestion centralisée et de mise en œuvre des stratégies, désactiver les processus en cours d'exécution associés à l'application coupable dans l'ensemble de l'environnement.
- **Visibilité** — McAfee Threat Intelligence Exchange est capable de surveiller tous les fichiers exécutables compressés et leur première exécution dans l'environnement, de même que l'ensemble des modifications survenant par la suite. Cette visibilité sur les actions effectuées par une application ou un processus depuis son installation accélère la réponse et la correction.
- **Indicateurs de compromission** — Il est possible d'importer des informations sur les hachages de fichiers dangereux, de manière à immuniser l'environnement contre ces menaces connues grâce à la mise en œuvre des stratégies adéquates. Si l'un des indicateurs déclenche une alerte dans l'environnement, McAfee Threat Intelligence Exchange peut bloquer tous les processus et applications associés à cet indicateur de compromission.

McAfee Web Gateway

Les téléchargements à l'insu de l'utilisateur (drive-by) et les URL malveillantes incorporées à des e-mails de phishing sont les principales méthodes d'attaque utilisées pour distribuer les logiciels malveillants sans fichier. **McAfee Web Gateway** est un produit robuste qui optimise la protection de votre entreprise contre ce type de menaces.

- **McAfee Gateway Anti-Malware Engine** — L'analyse des intentions sans signatures élimine, en temps réel, le contenu malveillant du trafic web. L'émulation et l'analyse comportementale protègent de manière proactive contre les attaques ciblées et de type « jour zéro ». McAfee Gateway Anti-Malware Engine inspecte les fichiers et empêche leur téléchargement s'ils sont malveillants.
- **Intégration avec McAfee GTI** — McAfee GTI propose une cyberveille en temps réel basée sur la réputation des fichiers, la réputation web et les catégories de sites web. Ces flux contribuent à assurer une protection efficace contre les dernières menaces, car McAfee Web Gateway bloque les tentatives de connexion à des sites web malveillants connus ou à des sites utilisant des réseaux publicitaires malveillants.

Outre ces produits Intel Security, nous recommandons deux autres technologies de sécurité.

- **Sécurité de la passerelle de messagerie** — La plupart des logiciels malveillants sans fichier compromettent les systèmes par l'entremise d'une pièce jointe à un message. Dès lors, une stratégie de défense bien conçue contre ce type d'attaques doit prévoir une solution robuste pour sécuriser la passerelle de messagerie.
- **Pare-feu** — La technologie de pare-feu est la pierre angulaire de tout système de sécurité. Un pare-feu peut détecter de nombreuses menaces au niveau du périmètre, avant qu'elles n'accèdent au réseau. Comme les logiciels malveillants sans fichier s'introduisent dans un système par l'intermédiaire de fichiers binaires statiques, bon nombre de ces attaques peuvent être bloquées avant qu'elles n'accèdent aux systèmes du réseau.

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

Intel et les logos Intel et McAfee sont des marques commerciales d'Intel Corporation ou de McAfee, Inc. aux États-Unis et/ou dans d'autres pays.
Les autres noms et marques sont la propriété de leurs détenteurs respectifs. Copyright © 2015 McAfee, Inc. 62193brf_fileless-malware_1215